Anti-Phishing Working Group

www.antiphishing.org

Fall 2008 Phishing Update
ICANN – ccNSO

Cairo, Egypt, November 5, 2008

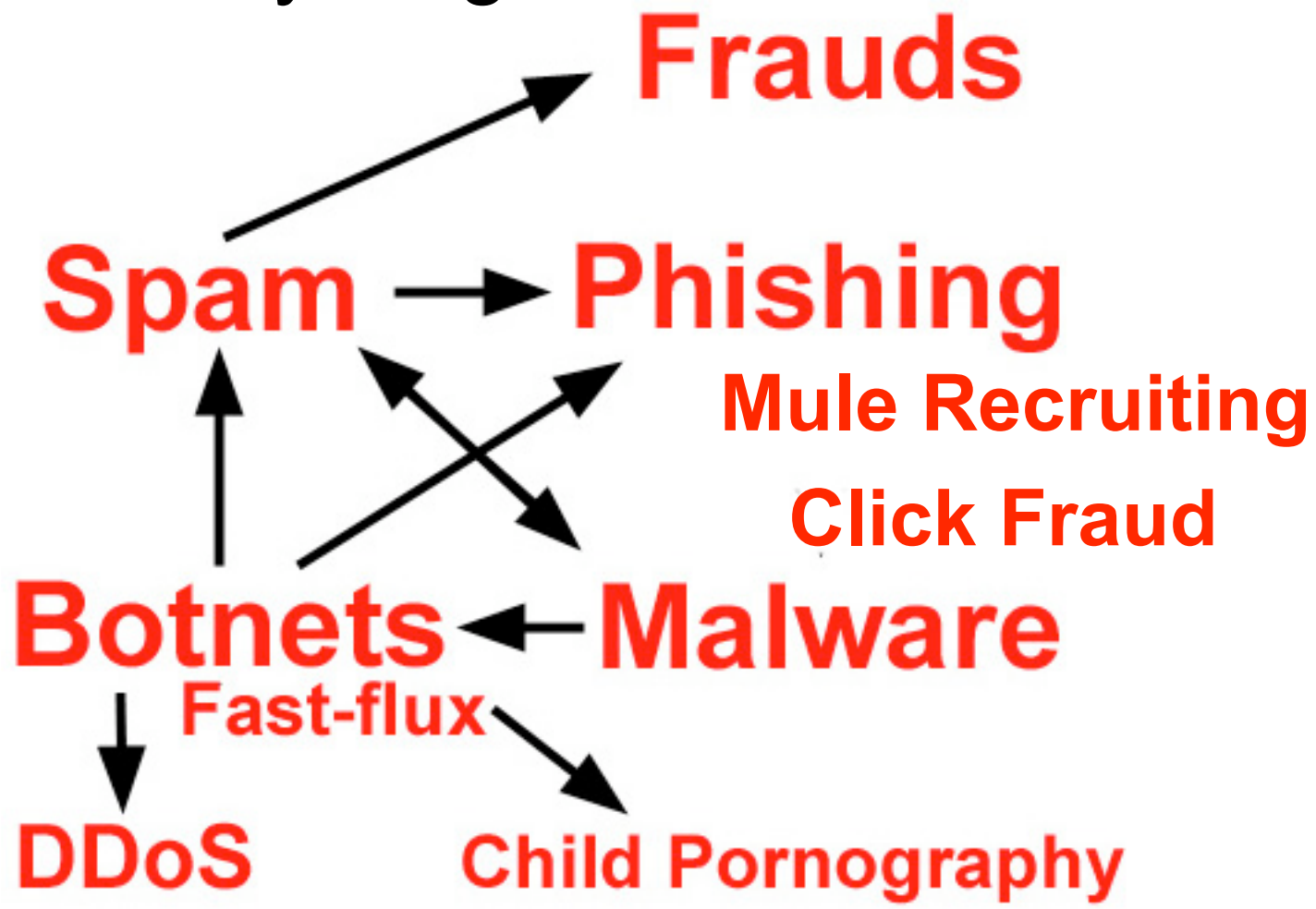
Rod Rasmussen
Co-Chair Internet Policy Committee of the APWG
President & CTO, Internet Identity

Dave Piscitello
Senior Security Technologist, SSAC

Topics

- Phish site education landing page
- New registrar phishing attacks
- APWG 1H 2008 phishing by TLD study results
- Live example - Venezuela
- Registry suspension plan status
- Registrar Best Practices document

Everything is Connected



Phish Education Page: The Goal

Consumer is educated at the “most teachable moment” – immediately after having been fooled by a phishing communication

How it works…

1. Investigators determine that a domain or URL is a phishing page
2. Offending page is taken out of service
3. Operators modify DNS or hosting server so that domain/URL resolves to Phishing education page
4. All would-be victims are protected and provided with a learning opportunity

The Page


APWG
Committed to wiping out Internet scams and fraud
www.antiphishing.org
Carnegie Mellon CyLab
Supporting Trust Decisions Project
cups.cs.cmu.edu/trust
WARNING!
The web page you tried to visit might have been trying to steal your personal information. That page was removed after being identified as a "phishing" web page. A phishing web page tricks people out of bank account information, passwords and other confidential information.
How You Were Tricked
This email is from my bank and is asking me to update my information. I better click on the link and update it.
STOP! Don't fall for scam email.
My Inbox
From: service@Wombank.com
Dear Jane,
Your account will be suspended if you do not update your information.
http://www.Wombank.com/update
How to Help Protect Yourself
1 Don't trust links in an email.
DANGER! http://www.amazon.com/update
2 Never give out personal information upon email request.
DANGER! Name: Jane Smith
Credit Card: 1234 5678 9101 1213
3 Look carefully at the web address.
http://www.amnazon.com
4 Type in the real website address into a web browser.
http://www.amazon.com
5 Don't call company phone numbers in emails or instant messages. Check a reliable source such as a phone book or credit card statement.
Credit Card Statement
For Customer Service call: 1-800 xxx-xxx
6 Don't open unexpected email attachments or instant message unload links.
My Inbox
Here is the updated document.
attachment

Text Version of the Page

Warning!

The web page you tried to visit might have been trying to steal your personal information.
The link you clicked to get here was probably created by con artists.

That page was removed after being identified as a "phishing" web page. A phishing web page is created to trick people out of bank account information, passwords and other confidential information.

Help Protect Yourself from Identity Theft

- Don't trust 'urgent' demands for personal information such as passwords in email or in instant messages.
  > **STOP.** Think. Avoid being rushed into giving up secrets or personal information you will later regret giving away.
- Don't trust links in email or in instant messages. They can lead to viruses and infect your computer.
  > **MANUALLY TYPE** the URLs for websites you need to visit, or use bookmarks you have created.
- Don't trust company telephone numbers in email or in instant messages.
  > **LOOK UP** telephone numbers using an established source. Use a telephone directory, a paper account statement or the telephone numbers on the back of your ATM cards and credit cards.
- Don't trust unexpected email attachments or instant message download links.
  > **SCAN** all attachments for viruses even in expected emails from friends and colleagues.

Legal Disclaimer

- PLEASE NOTE: The APWG. CMU's Supporting Trust Decisions Project and any cooperating service providers have provided this message as a public service, based upon information that the URL you were seeking has been involved in a phishing or malware exploit. There is no guarantee that you have not been phished or exposed to malware from this URL you were seeking, or previously. This is not a complete list of steps that may be taken to avoid

Text and image-rich pages will be translated into many languages

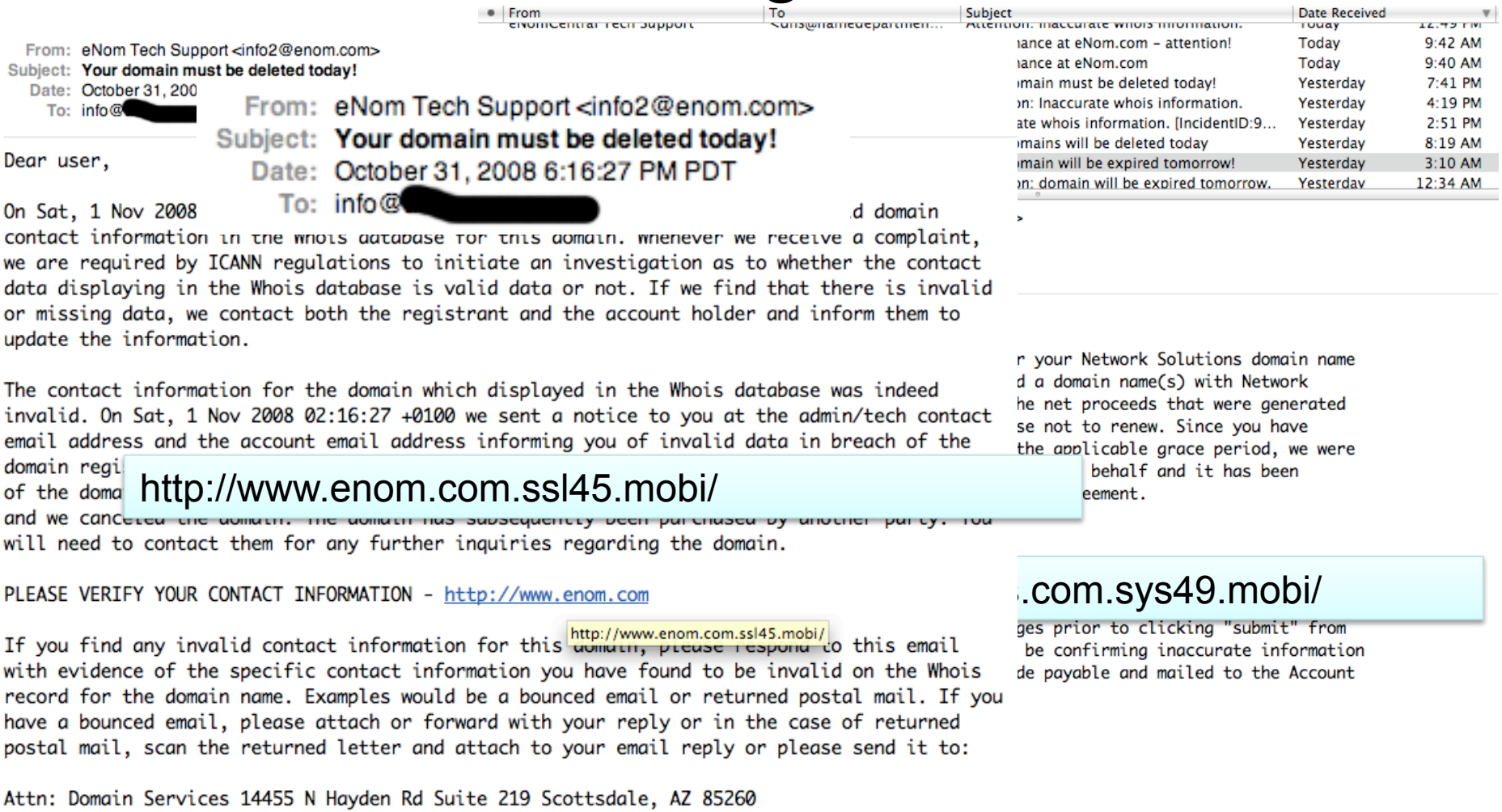
Questions for ccTLD Registries

- Can we enlist the help of domain registries to help recruit and support registrars to implement use of the landing page?
- Will you adopt usage yourself if your model allows it?
- Can you provide a standardized DNS location?
- Can you volunteer to assist in translation effort?

Phishing of Registrars/Registries

- ICANN phished after Paris meeting
- SOPHISTICATED attack launched this week
- eNom and Network Solutions targeted so far
- Threat REMAINS one of the largest potential disasters for the Internet and ICANN
  - Take over of a Financial Institution's domain portfolio through registrars' domain management systems
  - Majority of accounts still protected by username/ password only

Phishing Lures



From: eNom Tech Support <info2@enom.com>
Subject: **Your domain must be deleted today!**
Date: October 31, 200
To: info@[redacted]

From: eNom Tech Support <info2@enom.com>
Subject: **Your domain must be deleted today!**
Date: October 31, 2008 6:16:27 PM PDT
To: info@[redacted]

Dear user,

On Sat, 1 Nov 2008 .d domain contact information in the whois database for this domain. Whenever we receive a complaint, we are required by ICANN regulations to initiate an investigation as to whether the contact data displaying in the Whois database is valid data or not. If we find that there is invalid or missing data, we contact both the registrant and the account holder and inform them to update the information.

The contact information for the domain which displayed in the Whois database was indeed invalid. On Sat, 1 Nov 2008 02:16:27 +0100 we sent a notice to you at the admin/tech contact email address and the account email address informing you of invalid data in breach of the domain regi
of the doma
and we cancel
will need to contact them for any further inquiries regarding the domain.

PLEASE VERIFY YOUR CONTACT INFORMATION - http://www.enom.com

If you find any invalid contact information for this domain, please respond to this email with evidence of the specific contact information you have found to be invalid on the Whois record for the domain name. Examples would be a bounced email or returned postal mail. If you have a bounced email, please attach or forward with your reply or in the case of returned postal mail, scan the returned letter and attach to your email reply or please send it to:

Attn: Domain Services 14455 N Hayden Rd Suite 219 Scottsdale, AZ 85260

http://www.enom.com.ssl45.mobi/

http://www.enom.com.ssl45.mobi/

From | To | Subject | Date Received

Subject	Date Received	
ance at eNom.com – attention!	Today	9:42 AM
ance at eNom.com	Today	9:40 AM
main must be deleted today!	Yesterday	7:41 PM
n: Inaccurate whois information.	Yesterday	4:19 PM
ate whois information. [IncidentID:9...	Yesterday	2:51 PM
mains will be deleted today	Yesterday	8:19 AM
main will be expired tomorrow!	Yesterday	3:10 AM
n: domain will be expired tomorrow.	Yesterday	12:34 AM

r your Network Solutions domain name
d a domain name(s) with Network
he net proceeds that were generated
se not to renew. Since you have
the applicable grace period, we were
behalf and it has been
eement.

.com.sys49.mobi/

ges prior to clicking "submit" from
be confirming inaccurate information
de payable and mailed to the Account

Phishing Sites

Anti-Phishing Working Group

APWG

Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

Sophisticated attack vector

- The lures use many anticipated registrar messages (domain expires, whois update, errors)
- Fast-Flux based attack used10 IPs at once on various domains
- “Man on the side” data grabbing – unique attack
  - Use real code they scraped from the registrar site and use it as-is on their site
  - Use Javascript for a “simultaneous” request for a URL
- Data you enter into the phishing site actually posts to the real site too

Global Phishing Survey 1H2008

Greg Aaron

Rod Rasmussen

http://apwg.org/reports/APWG_GlobalPhishingSurvey1H2008.pdf

Data Set

- Comprehensive sources: APWG, phishing feeds, private sources, honeypots
- Millions of phishing URLs → small number of domain names
- Total of 167,638,848 domain names in the TLDs we have stats for. Accounts for ~ 99% of domain names in the world.
  - .cc, .to, .tv, .ph, .nu would be nice to get too!

Overall Stats

	1H2008	2H2007
Phishing on unique domain names:	26,678	28,818
IP-based phish (unique IPs):	3,389	5,217
TLDs phished on:	155	145
“Attacks”:	>47,342	
IDN domains:	52	10

Phishing by TLD: Scores

- Metric: “Phishing domains per 10,000”
- Measures prevalence of phishing in a TLD
- Median score: 2.3
- .COM score: 1.6
- Scores skew higher for smaller TLDs

Top 10 Phishing TLDs by Score

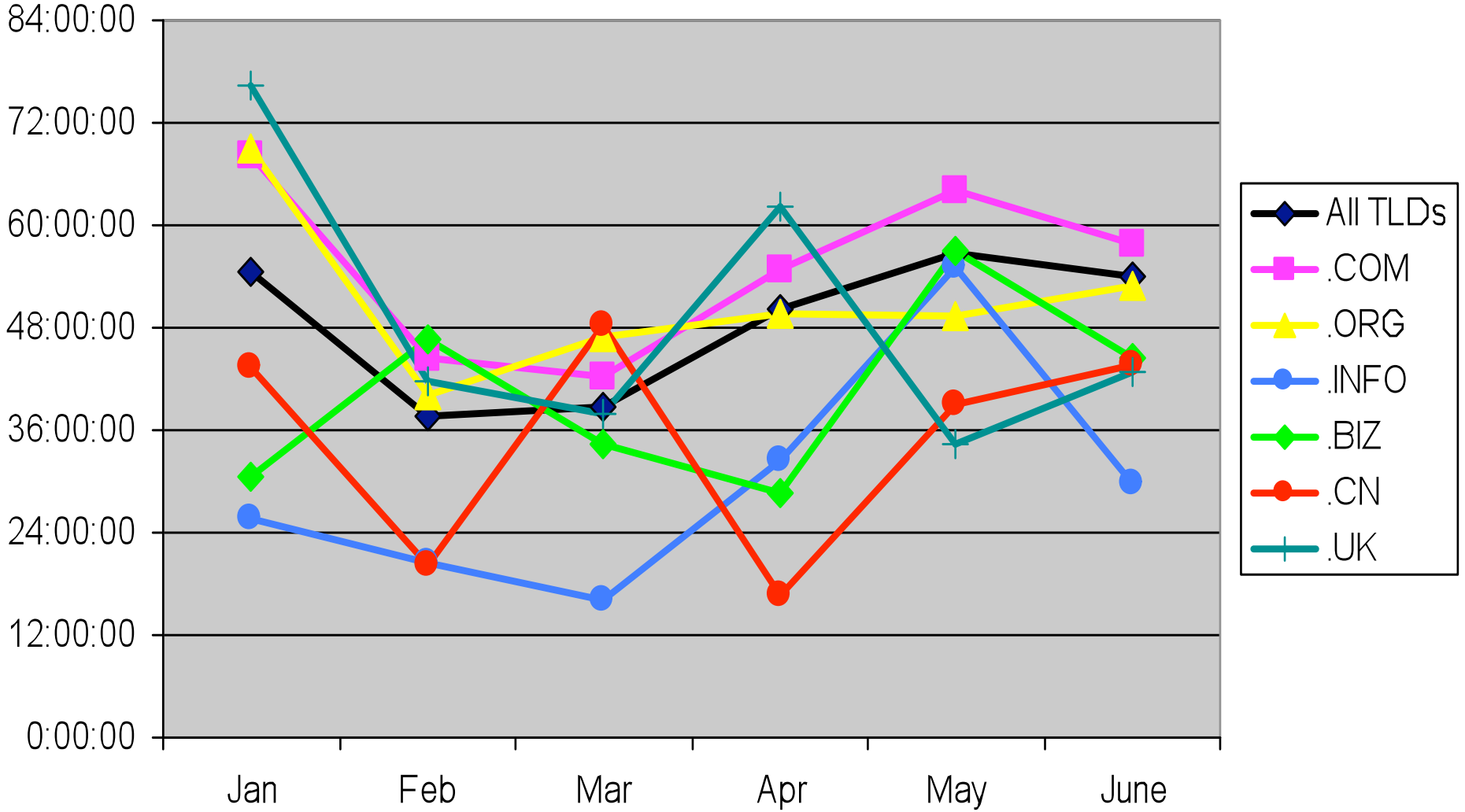
(minimum 30,000 domains and 25 phish)

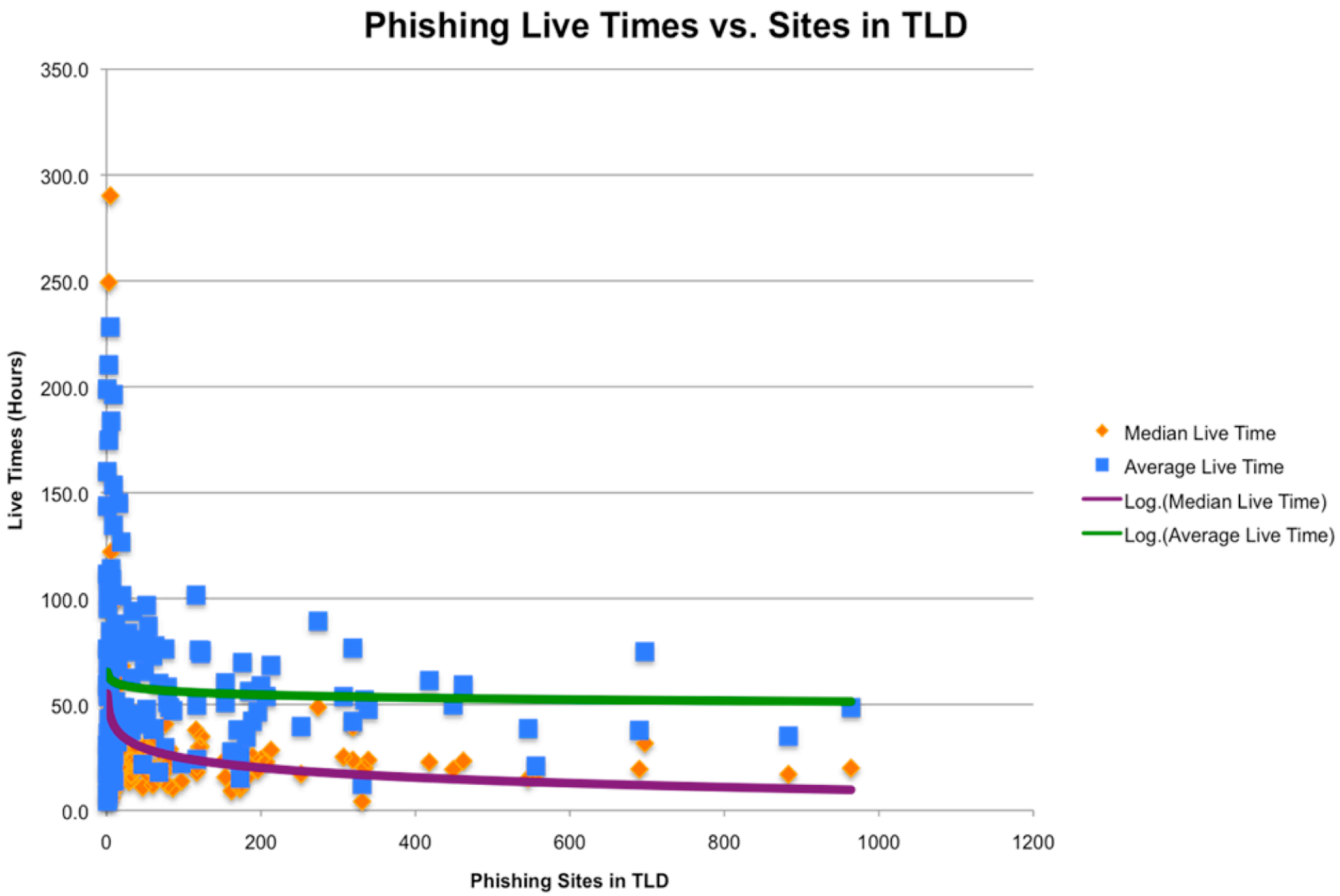
Rank	TLD	TLD Location	# Unique Phishing attacks 1H2008	Unique Domain Names used for phishing 1H2008	Domains in registry in May 2008	Score: Phish per 10,000 domains 1H2008
1	hk	Hong Kong	2,278	516	160,336	**32.2**
2	th	Thailand	154	84	35,757	**23.5**
3	bz	Belize	52	43	43,216	**10.0**
4	ve	Venezuela	86	71	75,000	**9.5**
5	cl	Chile	274	128	212,153	**6.0**
6	ro	Romania	184	142	284,700	**5.0**
7	li	Liechtenstein	97	26	59,546	**4.4**
8	name	sponsored TLD	331	126	289,343	**4.4**
9	tw	Taiwan	319	145	385,500	**3.8**
10	kr	Korea	697	345	945,000	**3.7**

Phishing by Uptime

- For 2008, gathering “live” times for phish
  - Automated monitoring of phishing sites
  - Check site status several times per hour. Site must stay down for at least 1 hour.
- Average and Median live times
  - Median is better barometer of how overall efforts are going
  - A few outliers that last weeks can vastly skew averages
  - Some stark examples between TLDs
- Overall stats:
  - All 51,500 attacks: median 19.5 hours, average 49.5 hours
  - 47,300 domain-based attacks: median 19 hours, average 49 hours 4,200 IP-based attacks: median 25.5 hours, average 59.5 hours

Average Phishing Uptimes 1H2008

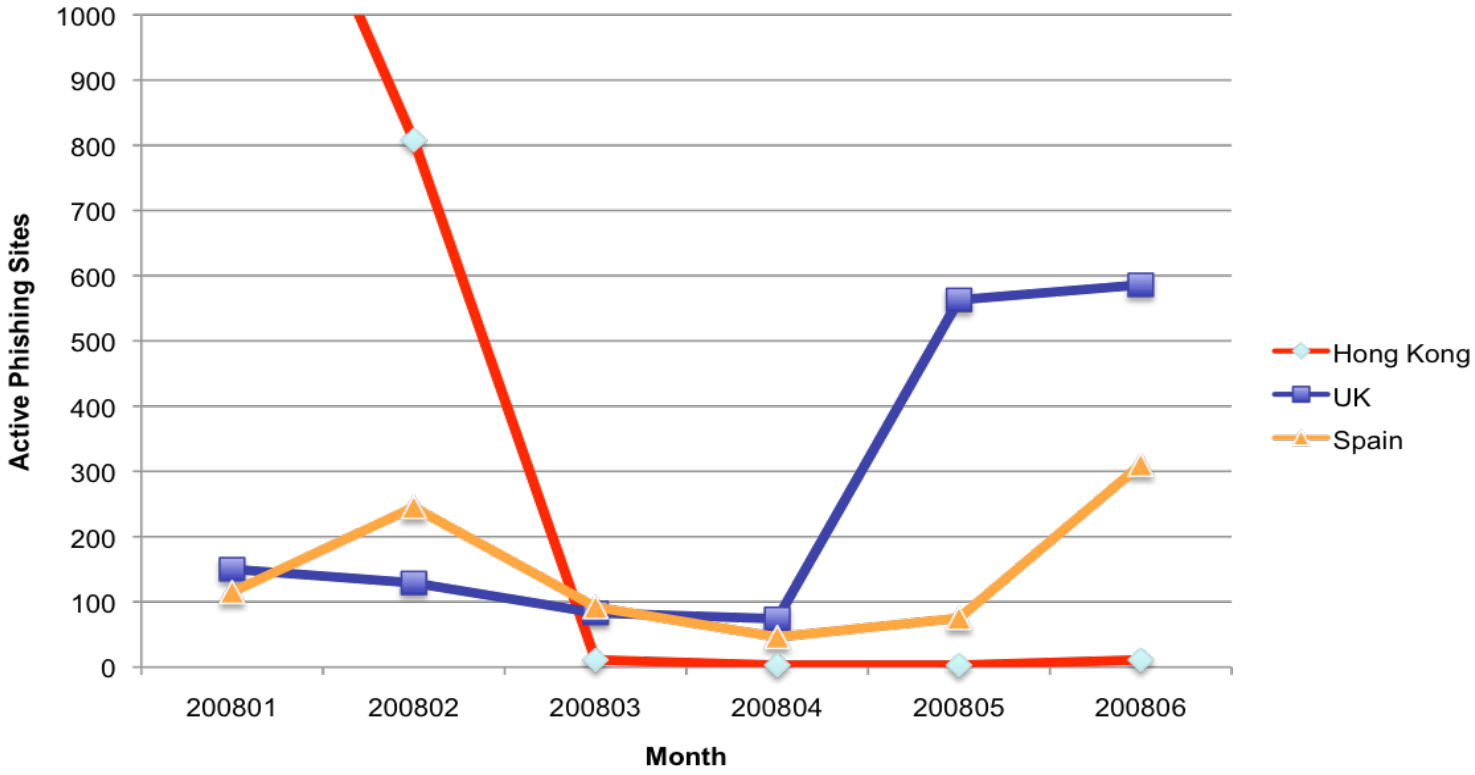



Phishing Live Times vs. Sites in TLD
Live Times (Hours)
350.0
300.0
250.0
200.0
150.0
100.0
50.0
0.0
0
200
400
600
800
1000
1200
Phishing Sites in TLD
Median Live Time
Average Live Time
Log.(Median Live Time)
Log.(Average Live Time)

1H 2008 GTLD Uptimes

TLD	Ave. Uptime Hours	Median Uptime Hours
.com	56:06	21:17
.net	48:09	20:51
.org	51:38	20:22
.info	25:13	15:24
.biz	38:35	15:05

Phishing attacks - Select TLDs targeted by ROCK Phish



Subdomain Services

- <customer_term>.<service_provider_sld>.TLD
- 4500+ subdomain sites/accounts on 274 unique second-level domains
- If we counted these as “domain names,” they would represent 9.5% of all domains
- For some TLDs, can greatly increase attack count
- Examples:
  - 379 phish on pochta.ru, 316 on land.ru, 251 on smtp.ru
  - 262 phish on ns8-wistee.fr, 250 on free.fr
  - 256 on 9k.com, 255 on altervista.org
- Up-times
  - Average: 45 hours, Median: 17 hours
  - Slightly better than overall numbers

Top 20 Subdomain Phishing Attacks

	Domain	Phish Sites	Domain Admin
1	pochta.ru	379	Pochta.ru
2	land.ru	316	Pochta.ru
3	ns8-wistee.fr	262	wistee.fr
4	9k.com	256	9k.com
5	altervista.org	255	altervista.org
6	smtp.ru	251	Pochta.ru
7	free.fr	250	free.fr
8	nm.ru	171	Pochta.ru
9	t35.com	142	t35.com
10	jexiste.fr	95	jexiste.fr
11	110mb.com	90	110mb.com
12	front.ru	82	Pochta.ru
13	krovatka.su	71	Pochta.ru
14	notlong.com	63	notlong.com
15	freeweb7.com	62	freeweb7.com
16	freehostia.com	60	freehostia.com
17	us.com	55	CentralNIC
18	de.com	45	CentralNIC
19	ifrance.com	44	ifrance.com
20	host.sk	40	host.sk

Top 15 Phishing TLDs by Attack Score

Rank	TLD	TLD Location	# Unique Phishing attacks	Unique Domain Names used for phishing	Domains in registry in May 2008	Score: Phish per 10,000 domains	Score: Attacks per 10,000 domains
1	hk	Hong Kong	2,278	516	160,336	32.2	**142.1**
2	th	Thailand	154	84	35,757	23.5	**43.1**
3	su	Soviet Union	154	14	60,543	2.3	**25.4**
4	li	Liechtenstein	97	26	59,546	4.4	**16.3**
5	ru	Russia	1,907	362	1,427,928	2.5	**13.4**
6	cl	Chile	274	128	212,153	6.0	**12.9**
7	bz	Belize	52	43	43,216	10.0	**12.0**
8	ve	Venezuela	86	71	75,000	9.5	**11.5**
9	name	sponsored TLD	331	126	289,343	4.4	**11.4**
10	fr	France	1,236	107	1,128,776	0.9	**10.9**
11	es	Spain	883	333	970,580	3.4	**9.1**
12	be	Belgium	690	62	791,737	0.8	**8.7**

Some Conclusions

Phishers are always adjusting and experimenting
- Moving from registrar to registrar, and TLD to TLD
- Moving away from using IP-based phishing

Use of domain names for phishing remained flat.

Still very little use of IDNs for phishing

Registry anti-abuse programs have an effect.

http://apwg.org/reports/APWG_GlobalPhishingSurvey1H2008.pdf

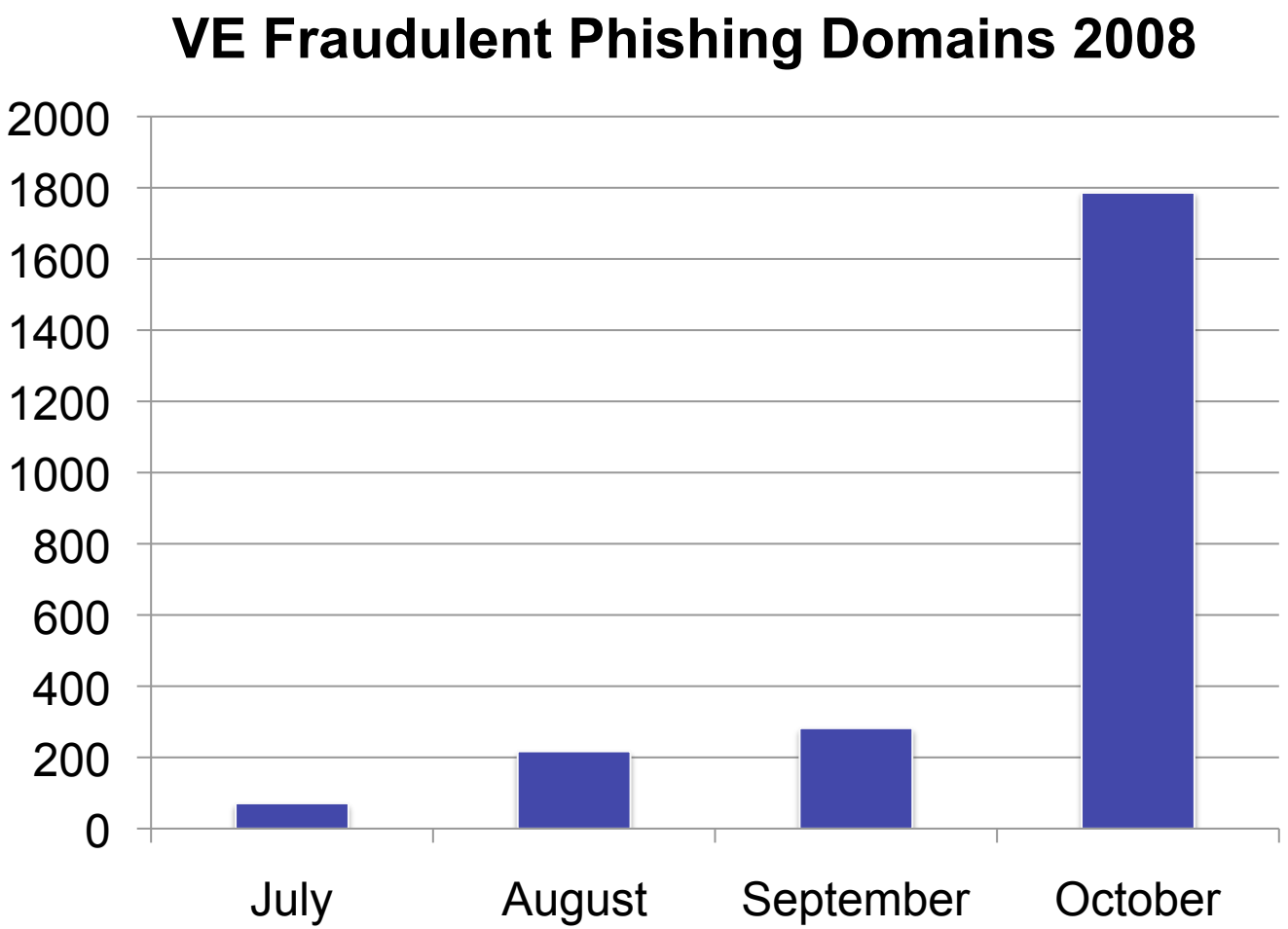
Venezuela: a Live Lesson

- TLD: .VE
- Combined Registry/Registrar Model
- Open registration policy
- Partial governmental control
  - Ministry in charge has changed in last few months
  - Indirect relationship to national police
- Prior to summer 2008 – very little phishing
  - Several domains in Feb-April 2008 but then a lull
- July 2008, new attacks start with a few sites
  - Register suspect names with all 6 sub-TLD variants
  - Initial response is pretty swift

Venezuela: Problems arise

- Process quickly breaks-down as dozens of domains are registered
- Work with registry to help them understand issues
  - Provide information on recent experiences of other registries (.HK primarily)
  - Coordinate with LACTLD
- Start to require “police directive” for shut-down
- Registry then claims they can’t suspend obviously fraudulent domains at all
  - Phishers start registering domains in the name of Donald Trump and “Internet Identity”
  - Registry STILL won’t suspend even though the take-down service is the registrant!

Ouch!


VE Fraudulent Phishing Domains 2008
2000
1800
1600
1400
1200
1000
800
600
400
200
0
July
August
September
October

Venezuela: What happened?

- NIC caught completely unprepared
- Stuck to policy rather than practical realities
- Take-down times dragged out to 2 weeks
- Phishers saw this
  - Vastly increased registrations
  - Taunted them/us
- Slow, bureaucratic path to change policy and process
- We may have a fix now – still waiting to see
- Ecuador (.ec) appears to be next in line…
  - We are working with LACTLD to try to come up with policy that all NICs in their region can utilize
  - We can really use your support on this effort!

Accelerated Domain Suspension Plan for Registries: Update

- .Asia expressed interest in getting this done and in place after recent .asia based phish
- We're a bit stuck
  - Accreditation agency to vet qualified interveners identified but will cost $$$
  - Interveners willing to pay, but need more bang for the buck
- So who else is willing to sign on to this idea?
  - Allows a registry to take active anti-abuse role within defined process and shared responsibility
  - Latest survey shows these efforts are effective

Registrar Best Practices

- Goal:
  - Cooperative effort between APWG and ICANN registrars
  - **Recommend** measures registrars can take to assist the anti-phishing community make the Internet safer for all
- Focus:
  - Evidence preservation (help LE catch the criminals)
    - What is useful? How to preserve? Who to provide to?
  - Registrant screening tips to identify fraud proactively
  - Phishing domain takedown assistance
  - Promote resources to help identify malicious activities
- Final version published at APWG site

Top Recommendations

1. *Timely response to domain take-down requests by shutdown authorities and/or law enforcement*
2. *Proactively use available data to identify and shut-down malicious domains*
3. *Share fraudulent domain registration information with law-enforcement*
4. *Protect registrar customers from being phished*
5. *Prohibit/minimize use of Fast-Flux Domains*

Other Recommendations

1. *Investigate domain registrations/name servers related to known criminal activity (i.e. if you know one domain has fraudulent aspects, find and eliminate others with the same)*
2. *Gather data used in bogus registrations for "scoring" future registration attempts*
3. *Update Acceptable Use Policy/Service Agreement – Cover yourself so you can eliminate bogus domains anytime*

APWG Contacts

- Website: http://www.antiphishing.org
- Phish Site Reporting: reportphishing@antiphishing.org
- Membership: membership@antiphishing.org

- e-mail
  - rod.rasmussen@internetidentity.com
  - Dave.piscitello@icann.org

Anti-Phishing Working Group

www.antiphishing.org

Fall 2008 Phishing Update
ICANN – ccNSO

Cairo, Egypt, November 5, 2008

Rod Rasmussen
Co-Chair Internet Policy Committee of the APWG
President & CTO, Internet Identity

Dave Piscitello
Senior Security Technologist, SSAC