

Anti-Phishing Working Group

www.antiphishing.org

Internet Policy Committee Initiative Update

Dave Piscitello, Sr. Security Technologist, ICANN
Policy Legate for the APWG



Committed to wiping out
Internet scams and fraud

APWG Internet Policy Committee (IPC)

- 50+ members
- Participants include
 - registries, registrars, ISPs
 - CERTs, Law Enforcement
 - solution providers, researchers, financial institutions, etc.
- Ensure that anti-phishing concerns are represented during the creation or modification of Internet policies

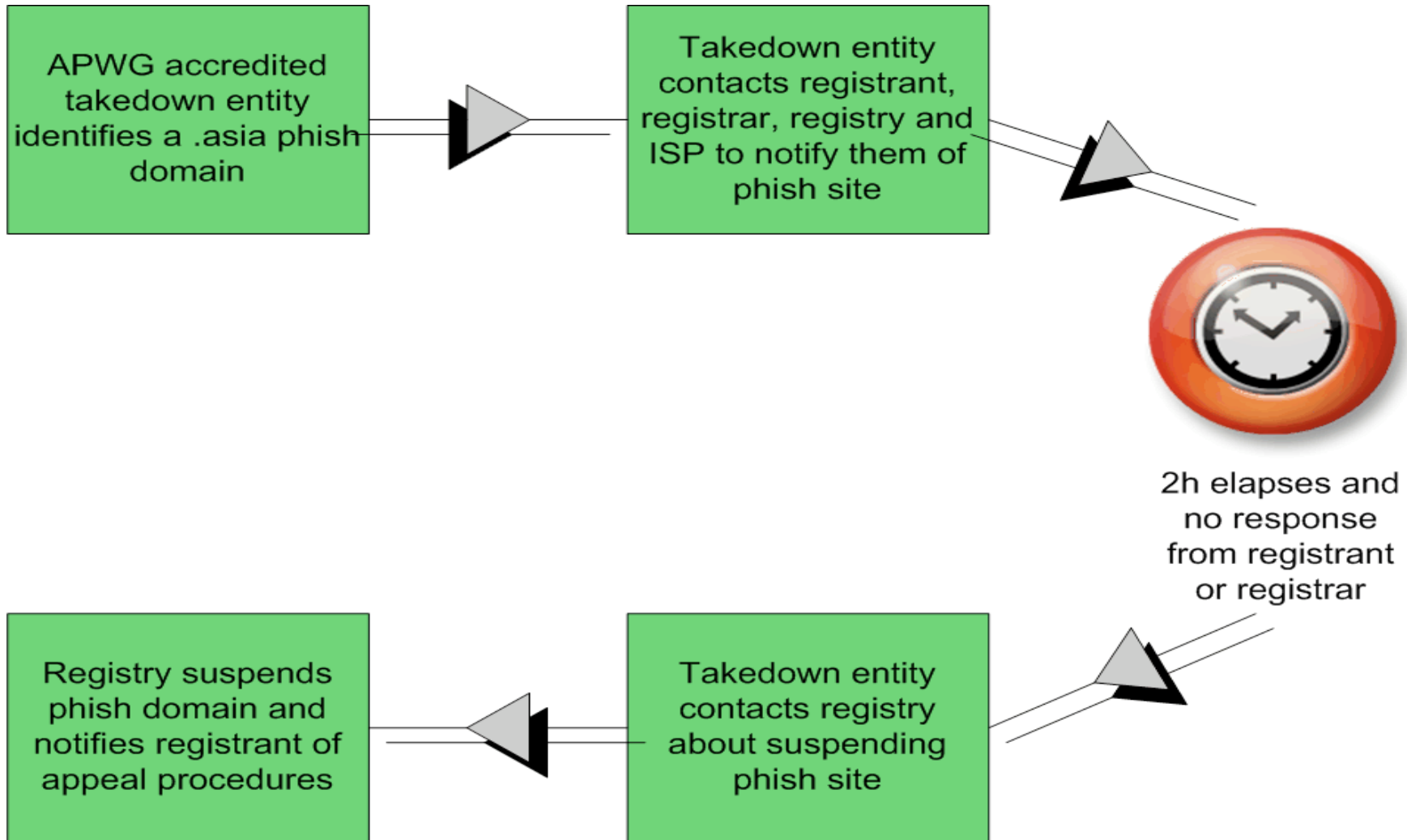
Initiatives

- Accelerated Domain Suspension by Registries
- Registrar Best Practices
- Phishing Site “Landing” page to educate victims
- Large-scale data study for 2007 phishing

Accelerated Suspension Plan

- Reduce site uptime of domains provably linked to phishing
- Define standard processes to suspend a phish domains
 - Assure small incidence of “false positives”
 - Hacked domains and shared hosting environments are not eligible for suspension
 - Appeal process and penalties for mistakes
- Establish APWG accredited entities
 - Trusted parties accredited by an agency chosen by a registry
 - Entities contact registry operators directly when registrar or registrant does not take action
- .ASIA and APWG formulating deployment plan

Accelerated Suspension Plan



Phishing Site Landing Page

- Use deleted phish URLs as an educational opportunity
 - Redirect people who fall for phishing lures to a page that teaches them how to avoid being phished
- Logistics
 - Hosted by APWG partner with hardened infrastructure
 - Available for use and “branding” by targeted FI’s
 - Text and graphical versions
 - Translated to multiple languages

The image shows a landing page for a phishing site, designed to educate users. At the top left is the APWG logo (www.apwg.org) and at the top right is the Carnegie Mellon CyLab logo (Supporting Trust Decision Project). A large speech bubble with a magnifying glass icon contains the word "Warning!" in orange, followed by the text: "The web page you tried to visit might have been trying to steal your personal information." Below this, a paragraph explains that the page was removed after being identified as a "phishing" web page and that the advisory is placed there to teach users how to reduce risks from phishing and online fraud. A section titled "Help Protect Yourself from Identity Theft" follows, with several "Do's" and "Don'ts" accompanied by small screenshots of phishing attempts:

- Do!** trust 'urgent' demands for personal information such as passwords in email, in instant messages or in cell telephone text messages. **STOP, Think.** Avoid being rushed into giving up secrets or personal information you will later regret giving away.
- Do!** trust links in email, in instant messages or in cell telephone text messages. They can lead to viruses and infect your computer, handheld device or cell telephone.
- Do!** trust company telephone numbers in email, in instant messages, in cell telephone text messages or even in CallerID displays.
- Do!** trust unexpected email attachments or instant message download links.
- Don't!** trust 'urgent' demands for personal information such as passwords in email, in instant messages or in cell telephone text messages. **DANGER!** ABC Bank Your account will be suspended if you don't update your information.
- Don't!** trust links in email, in instant messages or in cell telephone text messages. They can lead to viruses and infect your computer, handheld device or cell telephone. **DANGER!** Click here to log in: [http://www.abc.com/abc.com](#)
- MANUALLY TYPE** the URLs for websites you need to visit, or use bookmarks you have created. **www.abcbank.com**
- 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. **ABC Bank** For account inquiries call: 1-800-100-1000
- SCAN** all attachments for viruses even in expected emails from friends and colleagues. John: check out these pictures I took last weekend [mygallery.doc](#) Scanning attachment mygallery.doc 1 minute remaining...

<http://education.apwg.org/>

Registrar Best Practices

- Provide **recommendations** to registrars so they can play a stronger role in combating phishing
 - How to process and preserve evidence
 - How to offer effective registrant education
 - Phishing domain takedown assistance
 - Promote resources to help identify malicious activities
- Best practices have evolved into a broad initiative
 - Draft in review by registrars
 - gTLD and ccTLD operators forming group with registry focus
- Early success stories (HKDNR)
 - Implemented far better fraud-checking up-front
 - Improved policy surrounding domain suspension
 - Empowered support staff to handle domain suspension

Global Phishing Survey 2007

- Studies domain names and URLs to:
 - Measure scope of phishing problem world-wide
 - Understand what phishers are doing and why
 - Suggest anti-abuse measures
- Sources of data used in study
 - APWG, phishing feeds, private sources, honeypots
 - Millions of phishing URLs
 - 51,989 unique domain names plus 11,553 unique IP addresses

Compromised Domain or Malicious Registration?

- Compromised domain
 - Innocent (legitimate) site hacked by a phisher
 - Popular with phishers because they are hard to take down (“free” hosting, typically not blacklisted, ...)
- Malicious registration
 - Domain name was registered by a phisher
 - At least 20% of domains were maliciously registered
 - May be much higher

Trends in URL Construction

- Of the 10,773 maliciously registered domains:
 - 10,515 had the phish placed in subdomains or subdirectories
 - Only 258 had phish on “base” domain or home page
 - % of phishing URLs containing brand names increased in 2007
 - Phishers avoiding brand names in domain names
 - Brands in subdomains allows multiple phish per domain name
- Conclusions
 - Phishers don't care much what domain name they use. Any domain name (and any TLD) will do
 - To detect phish, study spam to identify phishing URLs and untrustworthy name servers.

Subdomain Services

- Phishers using subdomains of social networks or subdomain registries
 - <customer_term>.<service_provider_sld>.TLD
 - 11,443 subdomain sites/accounts on 448 unique second-level domains
 - Would represent 18% of all phishing domains if included in survey
- VERY difficult to take down
 - Most are free services
 - Mostly offered by small companies
 - No WHOIS
 - Spotty abuse resolution processing

Phishing by Top-Level Domain (TLD)

- 51,989 phishing domains
- 182 top-level domains (of 273) were phished
- Only 12 internationalized domain names (IDNs) used for phishing
- 150,689,751 total domain names in the 105 TLDs

Phishing by TLD: Scoring System

- New metric defined for this study
 - Phishing domains per 10,000
- Median score was 4.7
- .COM score 3.4
- Scores skew higher for smaller TLDs

Phishing by TLD: Top 10

(minimum 30,000 domains and 30 phishing incidents)

	TLD	TLD Location	Domains in registry in November 2007	Domain names used for phishing in 2007	Score: Phishing domains per 10,000
1	hk	Hong Kong	150,799	1,707	113.2
2	th	Thailand	33,000	171	51.8
3	li	Liechtenstein	50,100	221	44.1
4	ro	Romania	242,484	316	13.0
5	cl	Chile	195,513	222	11.4
6	bz	Belize	42,360	48	11.3
7	tw	Taiwan	341,462	361	10.6
8	lt	Lithuania	64,554	65	10.1
9	ee	Estonia	50,000	47	9.4
10	cz	Czech Repub.	347,989	286	8.2

Phishing by TLD: gTLDs

(Median Score for all TLDs = 4.7)

TLD	Domains in registry November 2007	Domain names used for phishing	Score: Phishing domains per 10,000
.ORG	6,412,064	2,627	4.1
.BIZ	1,944,453	764	3.9
.NET	10,581,849	3,973	3.8
.COM	70,698,420	23,860	3.4
.INFO	4,954,266	1,295	2.6

Low-Scoring Large TLDs

TLD	TLD Location	Domains in registry in November 2007	Domain names used for phishing in 2007	Score: Phishing domains per 10,000
cn	China	8,459,174	1,853	2.2
ws	Samoa	522,221	114	2.2
name	sponsored TLD	265,638	55	2.1
se	Sweden	685,000	127	1.9
ar	Argentina	1,451,727	230	1.6
de	Germany	11,524,091	1,798	1.6
uk	United Kingdom	6,445,465	992	1.5
eu	European Union	2,671,846	197	0.7
mobi	sponsored TLD	761,549	48	0.6

What Affects a TLD's Score?

- These factors make a difference
 - Registration requirements (citizenship, documentation)
 - Domain usage rates
 - Malicious registrations
 - Anti-abuse policies and procedures
- These factors do not
 - Registrant
 - Price
 - Registrar network

Malicious Registrations Make a Difference

TLD	TLD Location	Domains in registry in November 2007	Domain names used for phishing in 2007	Score: Phishing domains per 10,000
ly	Libya	3,100	84	271.0
mn	Mongolia	5,087	93	182.8
hk	Hong Kong	150,799	1,707	113.2
edu	U.S. education	6,997	67	95.8
th	Thailand	33,000	171	51.8
li	Liechtenstein	50,100	221	44.1

Conclusions

- Phishers are always experimenting
 - Are avoiding brand filters
 - Are systematically exploiting vulnerable registrars and registries over time
 - Are using subdomain services more often
- Phishers are TLD-agnostic
- Registries and registrars should concentrate on curbing malicious domain name registrations