eCrime Reporting Challenges

Patrick Cain

Resident Research Fellow

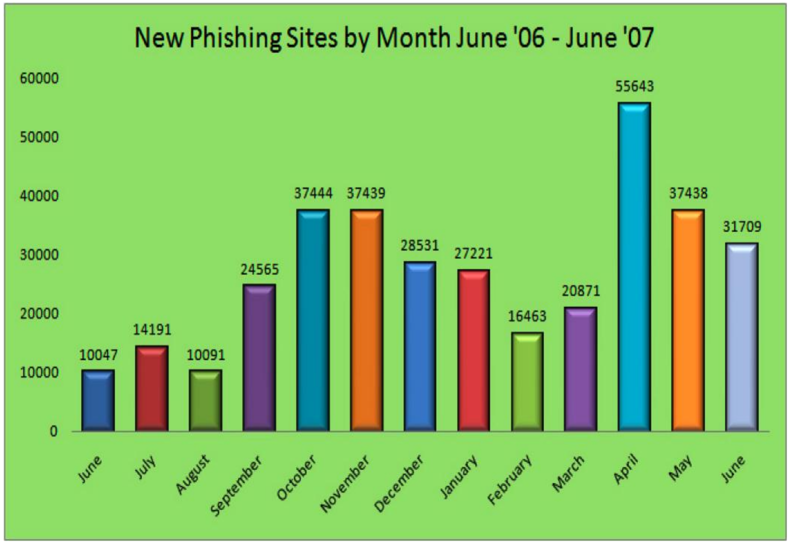
APWG

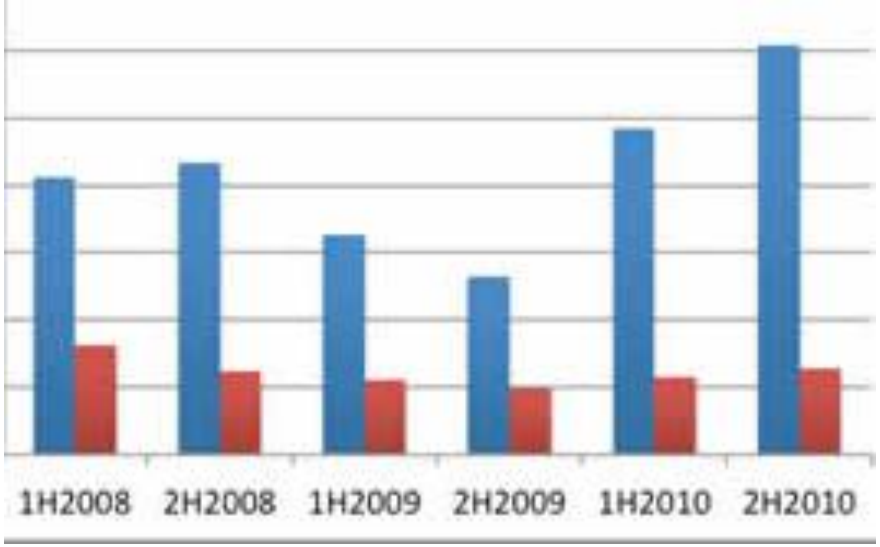
APWG Committed to Wiping Out Internet Scams and Fraud

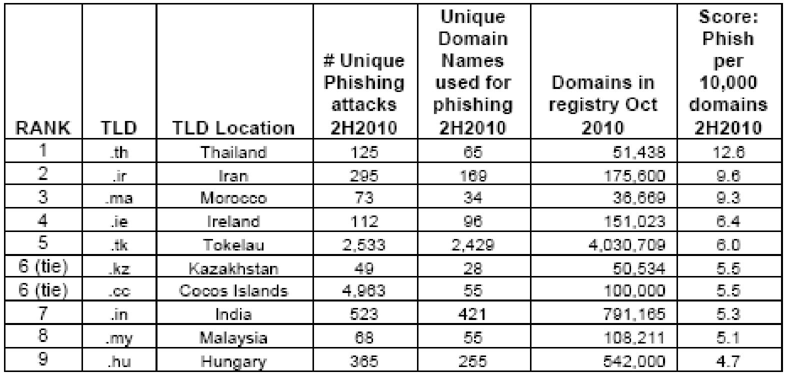
The APWG

- Started In 2004 as Anti-Phishing Working Group
- Non-profit CA corporation
- ~2100 members, 25 researcher groups
  - National Bodies, CERTs, LEA == free
  - Extreme International Composition
  - (Really) Big Company ←→ Sole Proprietor
- Many more non-members on open mail lists
- Goal: solve problems, share experiences and data
- Be vendor, country, and * agnostic

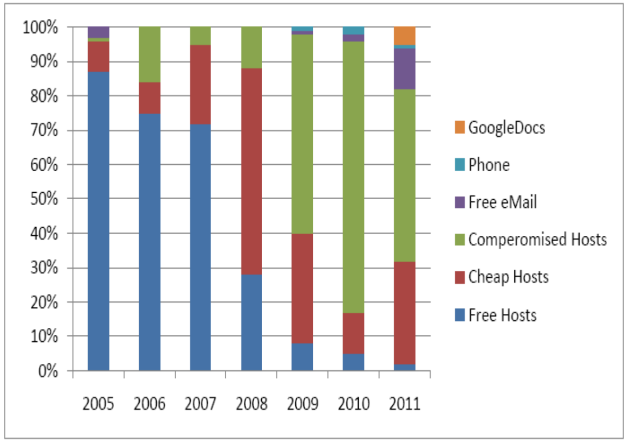
We Publish Statistics







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
1	.th	Thailand	125	65	51,438	12.6
2	.ir	Iran	295	169	175,600	9.6
3	.ma	Morocco	73	34	36,669	9.3
4	.ie	Ireland	112	96	151,023	6.4
5	.tk	Tokelau	2,533	2,429	4,030,709	6.0
6 (tie)	.kz	Kazakhstan	49	28	50,534	5.5
6 (tie)	.cc	Cocos Islands	4,963	55	100,000	5.5
7	.in	India	523	421	791,165	5.3
8	.my	Malaysia	68	55	108,211	5.1
9	.hu	Hungary	365	255	542,000	4.7



Committed to Wiping Out
Internet Scams and Fraud

We Hold Meetings

- Spring ‘Operations focused’ event
  - Rotates Internationally - EU, Asia, SA
    - Next month in Hong Kong
- Fall ‘Researchers Symposium’ in the US
  - In conjunction with the IEEE (and Research Advisors)
  - Accepted papers are published in an IEEE Journal
- Small, Spring European Researcher Summit
- Affiliated groups
  - Apwg.eu
  - Apwg.jp

In the beginning we collected ‘data’

- In 2004, we started collecting and sharing phishing URLs
  - Highly automated
  - Includes extra data (confidence, type of activity, etc)
  - Refreshed every 5 minutes
  - Entries time out after a few days
  - Errors can be corrected VERY quickly
  - List has between 30,000 and150,000 entries at a time
- We generate statistics on the collection
- There are multiple ways to send us data
  - Email. ftp, web GUI, etc
  - We do not operate data collectors – members and friends send us their observations

Then we moved to ‘events’

- This is really data aggregated to show patterns
  - E.g., brute forcing passwords, phishing campaigns, bot-infected systems, attack sources
- We use XML whenever possible to describe the event
- Developed the eCrime Exchange (ECX) to:
  - Get data; Put data; uses the data clearinghouse model
  - Explain your analysis of data; Talk about data
    - Goal: Make data analysis faster
  - Contains an automated notification facility
    - For ISPs, CERTS, etc for new data
    - For system owners if their systems are reported
  - Has a GUI for searching and examining
- Greatly increased the international participation

APWG Committed to Wiping Out Internet Scams and Fraud

Now moving to 'e-crime'

- Events aggregated for malicious activity
- A number of issues arose:
  - What is 'malicious activity'?
    - We need internationally agreed upon terms and definitions
  - Who do we report or notify?
    - National CERTS? ISPs? Police?
    - This isn't 'evidence', it's 'observations'
  - What specific data is needed by the receiver of the data

- We're rethinking the model of our data clearinghouse…

APWG Committed to Wiping Out Internet Scams and Fraud

Rethinking how we collect and share the datum

Framing the Engagement Model: The Organizing Question

- How does a world of localities engage the global cybercrime problem and respond as a unified, if virtual, enterprise?
- Traditional Models of Engagement
  - War Fighting?
    - Requires clearances, big money
    - Industrial/NGO responders are not soldiers
  - Law Enforcement?
    - Requires badges
    - Industrial/NGO responders are not police
  - Public Health?
    - The epidemiologic aspects of this model has some resonance with the challenges of engaging eCriminals
    - Definite maybe

How Does an Epidemiologic Response Model Work for Cyber Security?

- Public Health data collection & analysis is very similar to the way that cyber security firms collect, share and analyze cybercrime data
- Identification and quarantine procedures
  - Internet service providers emulate these practices for securing customers
- Remediation of outbreaks quickly after detection and diagnosis
  - Very important in both of these domains
- Imparting long-term hygienic principals that protect an individual and the public
  - An inoculation model of intervention

APWG Committed to Wiping Out Internet Scams and Fraud

Challenges in Using the Public Health Model for Fighting Cybercrime

- Private, not public, enterprises possess most of the event data that would inform epidemiologic models
- Private enterprise does not and likely will never have the authority to extract additional data, unlike public health agencies
- Cybercrime event data collection and exchange is impeded by regulatory, legal and apparent liability burdens
- Maximal results are attained when cybercrime event data collection and exchange happens at the speed of the crime itself
- eCrime responders and investigators need to be as good as the bad guys about sharing techniques and tips

APWG Committed to Wiping Out Internet Scams and Fraud

The Plan for Addressing the Challenges

- Develop cybercrime forensic response standards, protocols and resources to prioritize and coordinate interventions and investigations
- Organize a globalized response internetwork, or enable its development to reduce the eCrime infrastructure footprint
- Identify impeding areas in law/regulation and work with treaty organizations and governments to resolve conflicts with responder imperatives

No matter the model. things that still need work

- Useful data markings
  - Mark sensitive or not-sharable data subsets
- New consumable or supportable metrics
- Legal tweaks in data exchanges
  - Dealing with privacy is important
    - Especially in international contexts
- Sharing more data types in real-time

  CALAGI Polixenia
  - Malware distribution sites
  - Infected systems, C&C
  - Proxies and anonymisers addresses

Our Learned Lessons

- Sharing needs a level playing field
  - This is true for kindergarten; true for adults
  - Everybody signs the data sharing agreement (DSA)
    - What the receiver of the data can do with the data
    - Submittor expectations (resharing, publicity, marking, etc.)
- Data submission/retrieval needs to be easy
  - Nobody gets paid to send you data
    - Or to write the tools to move data
  - And automatic, or at least no human interaction necessary
- Normal operations need to be thought out
  - How do I fix errors & conflicts FAST
  - How to associate submittor feelings to recipient
  - How to get rid of DSA violators

Thank You

APWG Committed to Wiping Out Internet Scams and Fraud