New gTLD Program – Consultation Session on Trademark Protection & Malicious Behavior

24th June 2009
Hilton, Sydney

by
R.Azrina R.Othman
ISRAR Associates Sdn Bhd
MSc in Information Security & Computer Crime (Glamorgan University Wales, UK)
BSc in Computer Engineering (Lehigh University, USA)
SANS GCIA (2000-2008)
BSI BS7799 Lead Auditor
Co-founder of Malaysian Computer Emergency Response Team (MyCERT)

Agenda

- Threats & Issues
- Challenges
- Way Forward

Threats & Issues

- Domain purchase for phishing
- Bogus WHOIS data
- Unauthorized modification of NS records
- Domain squatting
- DNS fast flux for phishing and malware distribution host

Challenges

- ‘Broken window theory’ [1] – Inattentive subdomain providers, registrars and resellers attract bad actors in domain space.
- A particular service is used over and over, despite a good post-phish mitigation record
- CERTs and other phish fighters depend on WHOIS information to reach the rightful owner of domain names and IP Addresses in which information are not available or inaccurate
- Flagging on ‘bank’ names not sufficient to stop phishing
- Domain Dispute Resolution is too long a process for damage control

[1] APWG Global Antiphishing Survey 1H2008

Measuring Effectiveness

- Is it scalable?
  - Domain Lockdown – alert when registration initiated for domain used by Conficker, for example involves tens of thousands of domains daily to be monitored.
- Is security integrated into business process?
  - Cutting red-tapes at the expense of inflicted damage control
- Can the online process be abused?
  - Lack of verification & authentication process, anyone can steal email account and make changes to NS records.
- Does voluntary best practice works?
  - How to ensure responsiveness of registrars in responding to alerts and complaints?
  - Is the fast flux guide draw sufficient measures & how many adopt those measures?

Way Forward

- Reduce garbage in, garbage out
    - registries and registrars are in an excellent position to address malicious domain name registrations such as by tightening verification and authentication procedures for changing NS records

- Record owner of subdomain
    - To enable responders to contact the rightful party, subdomain service providers should provide valid contact records of owner of subdomain.

Way Forward

- Proactive scanning & detection
  - DNSMon, scanning to detect fast flux host and bots & sharing information among CERTs, LEAs, ISPs and registrars
- Reduce time for domain take down
  - Domain registrars play a crucial role in reducing the time phishing sites stay alive[1] . Implement enabling policy & processes. Establish circle of trust among key CERTs, LEAs, and relevant responders.
- Flag & act upon customers registering for malicious domains
  - Besides taking down domain, action such as investigation on the owner of the domain need to be initiated.

[1] APWG Global Antiphishing Survey 1H2008

Q & A