Top Trends in DNS Security

Dave Piscitello, ICANN
Rod Rasmussen, Internet Identity

Attacks against registration services

- Forms of attack
  - Socially engineer registrant or registrar staff
  - Exploit vulnerabilities in registrar web applications
  - Brute force authentication services
- Objectives
  - Gain access to a domain registration account
  - Modify DNS configuration to exploit name service
  - Cause reputational harm or facilitate other attacks
- Relevant SSAC documents
  - SAC028, Registrar Impersonation Phishing Attacks
  - SAC040, Measures to protect against registration service exploitation or misuse (publication pending)

Systemic abuse of registration services

- Criminals continue to find service providers to exploit heavily
  - Systematic testing of systems and responses
  - TLD, domain itself not important – want access to DNS
  - Will only relent once policies/procedures to curb are put in place by the provider
- Supports worst types of attack sites
  - Use fast flux and other techniques to keep sites live
  - Most prolific spammers and highest victimizations
- Relevant APWG Documents (at http://apwg.org)
  - Anti-Phishing Best Practices Recommendations for Registrars
  - Global Phishing Survey: Domain Name Use and Trends

DNS Wildcarding, Redirection, Synthesized Responses

- Return a positive response to a DNS query when a negative response is expected
  - Wildcards in TLD zone files (Sitefinder)
  - Response modification by entrusted DNS provider
  - “On the fly” modification of NXDOMAIN response
- Affects more than just web applications
  - Monitoring and management applications need to see errors
  - Zone authority loses control over delegated name space
- SSAC documents
  - SAC032, DNS Response Modification
  - SAC041, Recommendation to Prohibit use of Redirection and Synthesized Responses in New TLDs

Botnets

- Global pandemic
  - Infections in every country
  - Conficker: Domain abuse in 100s of TLDs
- Malware removal is hard
  - Malware writers quickly modify malware and variants in response to security and DNS community actions
- Conficker operational response proved that botnet activity can be “contained”
  - Time to consider models in which security and DNS communities can be proactive as well as reactive

Subdomain registration services

- Subdomain registration is popular in CCTLDs
  - Usually free or low cost hosting with DNS service
    - Format: registered-label<dot>domain<dot>tld
    - Example phish domains:
    - signin.ebay.pochta.ru, wellsfargo.ns8-wistee.fr
  - More than web
    - blogs, pictures, hosting, social networks and **email**
  - Operates outside ICANN or CC authority remit
    - No WHOIS, no zone file access, ad hoc suspension process

Subdomain registration services

- Criminal use of subdomain services on the rise
  - Abusive subdomains nearly as prevalent as phish domains
    - 6,300+ subdomain sites/accounts on 480 unique second-level domains
    - Increased nearly 50% over 1H2008, adding 200+ new unique second-level domains
    - If we counted these as “domain names,” they would represent 12% of all domains
  - Major impacts on specific TLD abuse levels
- Relevant APWG Documents (at http://apwg.org)
  - Making Waves in the Phisher’ Safest Harbors: Exposing the Dark Side of Subdomain Registries
  - Global Phishing Survey: Domain Name Use and Trends

APWG global phishing survey 2008-2H

- Phishers move from registrar to registrar, TLD to TLD, to exploit the best phishing “holes”
- Moving away from IP-based phishing
- Registry anti-abuse programs have an effect
- Of the 30,454 phishing domains, we identified 5,591 (18.5%) clearly registered by phishers.
  - Of those 5,591, only 1,053 domains contained a relevant brand name or misspelling. (Only 3.5% of all domains used for phishing.)
  - Majority of phishing sites set-up on compromised servers
- Phishers happy to use any domain name

Top 10 Phishing TLDs by Score

(minimum 30,000 domains and 25 phish)

Rank	TLD	TLD Location	Unique Domain Names used for phishing 2H2008	Domains in registry in Dec 2008	Score: Phish per 10,000 domains 2H2008
1	ve	Venezuela	1,504	82,500	**182.3**
2	th	Thailand	88	39,880	**22.1**
3	bz	Belize	55	43,377	**12.7**
4	su	Soviet Union	76	85,119	**8.9**
5	ro	Romania	188	310,114	**6.1**
6	cl	Chile	116	232,897	**5.0**
7	kr	Korea	413	983,626	**4.2**
8	vn	Vietnam	37	92,992	**4.0**
9	ru	Russia	676	1,860,179	**3.6**
10	tw	Taiwan	144	406,669	**3.5**

Questions and Discussion