Measures to Protect Domain Registration Services against Exploitation or Misuse

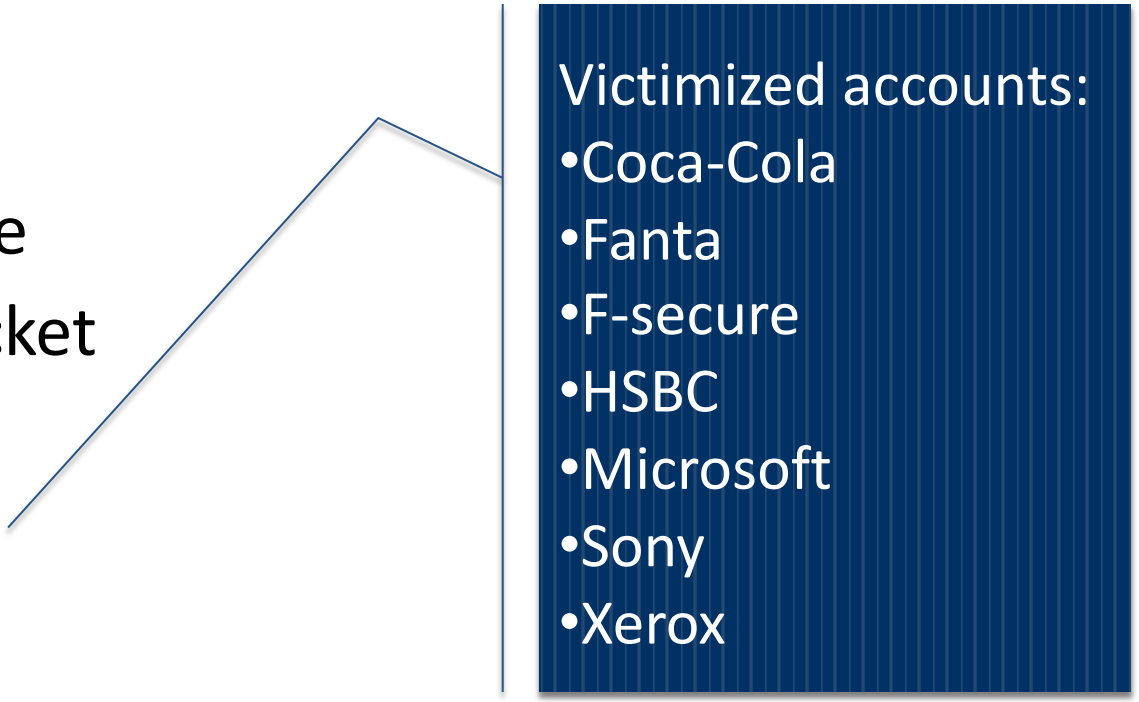
June 2009

Dave Piscitello

ICANN SSAC

What instigated this work?

- Attacks against domain registration accounts and registrars
  - ICANN
  - Comcast
  - CheckFree
  - Photobucket
  - RedTube
  - DomainZ



Public reaction to incidents

- “another reminder of the fragility of the net's domain name system” - The Register May 2008
- “Remember the DNS hijackings last year? Similar incidents are still happening.” - ZDNet April 2009
- “a potent reminder of the fragility of the internet's routing system. In this case, a small portion of it was compromised by a single web application error.” - The Register April 2009
- “registrars are often the weakest link and an easy target for attackers who want to hijack high profile web sites”

- Zone-H Report April 2009

What do these incidents reveal?

- All an attacker needs to gain control of an entire domain name portfolio is a user account and password
  - Guess, phish, or socially engineer a single point of contact
  - Attackers also scan registrar account login portals for web application vulnerabilities
  - Attacker can change contact and DNS information of **all** domains in the account
- Email may be only method registrar employes to notify a registrant of account activity
  - Attackers know this and block delivery to registrant by altering DNS configuration
- Recovery from DNS configuration abuse is slow

Findings

- Attackers exploit password-based authentication to gain access registration accounts
  - Compromise exposes all domains in account to attack
  - DNS configurations are favorite targets
- Unconfirmed email is an unreliable method for delivering notifications to registrants
- Security measures vary among registrars
  - Customers need more information to make informed decisions when choosing a registrar
- Domain name account access should be as secure as an e-banking or e-merchant transaction

Threats against registration service are not unique

- Consider financial institutions, e-merchants, corporate intranets and extranets
  - Similar threat models
  - Similarities in scale and diversity of customers
  - Same benefits derived by educating customers and distinguish service offerings from competition
- What measures do they take to counter these threats?
  - Multi-factor authentication methods
  - Endpoint verification
  - Granular access controls to customer data
  - Diversity in customer correspondence methods

Registrars can follow suit

- Improve “security baseline” for all registrants
- Differentiate by offering better-than-baseline security for customers who want more
- Make customers aware of security features so they can make informed choices
- Use security to attract customers
  - Voluntary security auditing by trusted 3rd party or
  - Secure registrar seal or trusted mark program
    - Same motivation and principles as ICANN accreditation or SSL trusted security marks

Recommendations

- Registrars: offer more protection against registration exploitation or misuse
  - Improve the baseline service for all registrants
  - Consider offering better-than-baseline service
- Registrars: make information describing measures to protect domain accounts more accessible to customers
- Registrars: consider an independent security audit as a component of self-imposed security due diligence
- ICANN: consider whether a trusted security mark programs would improve registration services security

Next Steps

- Collaboration with registrars (ICANN Sydney)
- Publication of SAC040, Measures to Protect Domain Registration Services against Exploitation or Misuse (July 2009)
- SSAC call for public comment