Protecting High Value Domains

SSAC Public Meeting
ICANN Cairo 2008
What is a high value domain?

• Working definition: high value domain (HVD)
  – One or a set of names which define an organization's online presence
  – A domain an organization expects to register “forever”, without interruption
  – A name the organization cannot do without!
  – A domain that is an attractive, “high profile” target for hijacking or attacks
Attacks against High Profile, High Value Domains

• Comcast.net hijacking
  – Attacker impersonated Comcast technician, convinced registrar support staff to reset account password
  – Attacker used DNS hosting to modify zone, redirected traffic to web defacement, interrupted web mail services

• ICANN
  – Attacker gained control of domain account via ICANN's registrar's systems
  – Attacker redirected traffic to protest web page

• Paypal.com
  – Ebay (parent company) sought help from registrar to take down phishing domains. Paypal.com taken out of service as a result of registrar error
Why is SSAC interested in HVDs?

- Registrars are no less prone to errors than other businesses
- What curative measures could prevent repeat incidents involving other high profile, high value customers?
- Are protective measures available from registrars, registries, and the registrant's IT or outsourcing agent
  - Sufficient?
  - Available to as broad a range of registrants as need them?

![Diagram showing need, want, can afford, and cannot afford categories]
Scope of SSAC Study

• Conduct interviews with
  – Attack victims (registrants and registrars)
  – Registrars that offer extra protective measures for domain name portfolio holders
  – Medium-sized and large organizations with HVD portfolios

• Examine existing and candidate measures to
  – Protect against unauthorized access
  – Protect against unauthorized transfers
  – Protect against internal staff or process errors (and bad acts)
  – Provide avoidance mechanisms to prevent non-renewal or deletion of domain name
  – Protect against DNS configuration abuse
  – Maintain registration information accuracy and integrity
Two registration service models exist today

- Basic registration services
  - Oriented to consumers
  - Emphasis on high transaction rates
  - Automated processes
  - Human intervention for exception handling

- Extra (premium) protection services
  - Protective measures are part of a broad package that emphasizes brand equity protection
  - Emphasis on handling individual transactions with low probability of error
  - Human assistance or confirmation is often mandatory
Models for Managing HVDs

• Asset and risk management
  – Domain names are assets
  – Customers must consider threat model

• Provisioning management
  – Domain names are critical to network operations and business applications
  – Primary operations are \{add, drop, change\}

• Primary objective of customers with HVD is protection against loss and misuse of assets
  – Add (to portfolio) is frequent, drop is rare
  – Change may occur frequently
    • Was the change expected or is it indicative of an attack?
Protecting access to domain portfolio

• Possible measures for the registrant
  – Identify multiple portfolio administrators
  – Include contacts in Employee Resource Management process
  – Self-impose a password change policy
  – Periodically verify contacts
  – Use a separate domain for registration contact email accounts (role accounts) from domains used for other business purposes
Protecting access to domain portfolio (2)

• Possible measure for registrars to offer (business opportunities not policy recommendations)
  – Enforce multi-factor authentication
  – Require multiple, unique identities as contacts in registration records
  – Require confirmations of change from multiple contacts using email, possibly via media other than email
  – Notify multiple contacts subsequent to implementing a change (possibly different or broader set than parties with change authority)
Preventing loss of domains (transfer, non-renewal, deletion protection)

• Possible measures for the registrant
  – Proactively monitor domain name registration
  – Treat transfer attempts as a security event (check and re-check)

• Possible measure for registrars to offer (business opportunities not policy recommendations)
  – Registrar lock
  – Issue transfer and non-renewal notifications to multiple contacts via multiple delivery methods
  – Require multi-factor proof of identity and role from registrant, administrative and technical contacts
  – Require confirmations of change from multiple contacts using email, possibly via media other than email
  – Safeguards against internal threats or processing error
Protecting DNS configuration

• Possible measures for the registrant
  – Monitor DNS configuration activity
  – Maintain DNS configuration history for domains

• Possible measures for the registrar
  – Require multi-factor authentication for DNS changes
  – Require confirmations of change from multiple contacts using email, possibly via media other than email
  – Deliver notifications to multiple contacts when changes performed
  – Monitor DNS changes for anomalies or abuse
  – Safeguards against internal threat or configuration error
Room for a 3rd business model?

Today

Future

Nominal

Considerable

Protection

Considerable

Protection

COST

$1000s

$1s

Nominal

Considerable

Protection

COST

$1000s

$1s

Nominal

Considerable

Protection

COST

$1000s

$1s

Nominal

Considerable

Protection

COST

$1000s

$1s

Nominal

Considerable

Protection
Next steps

• Continue to interview HVD owners and registrars who offer extra protection services
• Interview small and medium-sized businesses who could benefit from affordable extra protection services
• Discuss feasibility of broader range of protective measures "offerings" with registrars and resellers
• Report on findings