ICANN 59
POLICY FORUM
JOHANNESBURG
26–29 June 2017

Security Trends Impacting Registrants
27 June 2017

Outline

1
Security Trends Impacting Registrants

2
What can Registrants Do?

3
Q & A

Security Trends Impacting Registrants

Threats Impacting Registrants

External Threats

- Attackers seeks to gain unauthorized access to domain name registration account to control ("hijack") a domain name
- Attackers seeks to gain unauthorized access to domain name registration account to alter DNS information associated with the domain name

Internal Threats

- A party interested in your domain name closely monitor the name as registration nears expiration and register the domain name if the registrant forgets to renew.

Unauthorized access to domain registration account

- Domain registration accounts are vulnerable to many forms of attacks
  - Guess attack
  - Capture from a host containing credentials
  - Capture them as they are entered
  - Social engineering (phishing, spear-phishing)
  - Attacking the registrar/registry directly

Unauthorized access to domain registration account

Account compromise usually precursors to:

- Malicious or unintentional alternation of DNS Configuration Information
  - Changes to DNS configuration results in resolution of names to IP address other than the addresses registrant intended.
  - Result in loss or disruption of service (web, email), redirection to attack server
  - Lack of coordination or administrative error can introduce changes with similar consequences

Unauthorized access to domain registration account - cont.

Account compromise usually precursors to:

- Malicious or unintentional alternation of contact configuration Information. Could result in:
  - Transfer or wrongful taking control of a domain name (hijacking)
  - Disruption of service delivery of registrar correspondence
  - Filing of a report of WHOIS inaccuracy against the registrant that leads to suspension or deletion of domain name
  - The deletion of a domain name registration by the unauthorized party

Failure to renew a domain name registration

- Renewal lapse occurs when by choice or oversight, a registrant allows a domain name registration to expire.
  - A different party register the domain name after the expiration of relevant grace periods.
  - In some cases, the new registrant prove harmful to the interests of the old.
  - The old registrant have to absorb the switching cost or pursue a time consuming dispute resolution process

What Can Registrants Do?

Actions For Registrants - I

- **Consider domain name registration as an asset** and included in business processes such as asset management, provisioning and risk management programs
  - A domain name registration deserves the same rigor as other sensitive digital or physical assets.

Actions For Registrants - II

Protection Against Unauthorized Access

- Protect Account credentials
- Take advantage of routine correspondence from registrars
- Maintain documentation to “prove registration”
- Use Separate identifies for registrant, technical, administrative, and billing contacts
- Incorporate registrar email correspondence into domain management
- Identify domain name registration points of contact by role
- Add diversity to email contacts to reduce single points of failure of attack, and keep key email accounts secure.
- Improve change control and coordination
- Maintain accurate external contacts

Actions For Registrants - II

Measures to Detect or Prevent Unauthorized Change Activity

- Monitoring for WHOIS change activity
- Monitoring DNS change activity
- Setting and Monitoring Domain Status (Domain Locks)
- Choose the Domain Registration Service Provider carefully

Further Reading

- SAC074: SSAC Advisory on Registrant Protection: Best Practices for Preserving Security and Stability in the Credential Management Lifecycle (03 November 2015)
- SAC044: A Registrant's Guide to Protecting Domain Name Registration Accounts (05 November 2010)
- SAC040: Measures to Protect Domain Registration Services Against Exploitation or Misuse (19 August 2009)
- SAC010: Renewal Considerations for Domain Name Registrants (29 June 2006)

Questions and Answers