DNS Hijacking

Inappropriate domain name management causes DNS Hijacking

CENTR Paris
July 31, 2005

Kazunori Fujiwara
<fujiwara@jprs.co.jp>

What is ‘inappropriate domain name management’?

- Registrants have to manage:
  - DNS servers that provide zone information (Child)
    - Contains DNS servers’ information
  - DNS servers’ information registered to registry (Parent)
- Child and Parent should be synchronized
  - If not, it causes lame delegation
  - If not, it is one of inappropriate state
- Typical inappropriate states
  - Registering wrong name (typo)
  - Leaving expired (non existing) name
  - Leaving non working DNS server

- These states may cause DNS hijacking.

How ‘domain name hijack’ can happen?

- Suppose DNS server’s domain name registered to registry do not exist.
  - example: EXAMPLE.JP has NS1.EXAMPLE.JP and NS2.NOEXIST.TLD
    - NOEXIST.TLD was expired and not exist.
  - Someone can register NOEXIST.TLD and setup NS2.NOEXIST.TLD as DNS server.
  - Then someone can forge zone information.
    - DNS responses from NS1.EXAMPLE.JP and NS2.NOEXIST.TLD are different.
- The situation easily happen.
  - If communication between domain name registration managers and DNS operation managers are not smooth in registrant organization.

A case study in Japan

- One domain name had two DNS servers in May 2005
  - Credit card company’s domain name.
  - One DNS server works and the other is stopped.
- But stopped DNS server’s domain name was expired and anyone could register it.
  - An attacker could register the domain name and run malicious authoritative DNS server.
  - In this situation, phishing was easy.
- One person warned this issue to Japanese community.
- Now, it has been corrected.
- IPA (a governmental organization) announced a security advisory about this issue.
  - After that, JPRS, JPCERT, and Ministry of Internal Affairs and Communications announced advisories.
  - Various web media published it.

Whose responsibility?

- Domain name management is done by the responsibility of ″Domain name registrant″.
  - Registrant should confirm and correct mistakes.
  - TLD accepts registration demands as it is from Registrants or Registrars.
- Meanwhile, registries/registrars can observe inappropriately managed domain names easily.
  - What registries can offer?
  - Registries should make an effort to offer the appropriate setting.

TLD’s possible choices.

- Promote Registrants’ understanding about DNS.
  - Web pages of registries/registrars/ISPs/…
  - News from media
  - Public Lectures
- Check the status of domains and warn the registrants/registrars whose domain registration is inappropriate
  - Only TLD registries can check all domains.
  - But DNS server name check is difficult if registered DNS server name is outside the TLD.
  - Cooperation between registries is required.
- Remove DNS server registration if the domain name is exposed to significant danger.
  - With or without any notification

JPRS’ action

- Expressed public warning on the Web site
- Checked unmanaged domain names inside .JP
  - DNS servers of another TLDs are not checked
- Sent warning mails to registrars
- Will send warning to registrants
  - Planned next week

Today’s discussion

1. What should we do as TLD registry?
   1. What should registrars do?
   2. What should ISPs do?
   3. What should registrants do?
2. Possibly, sharing of code of conduct/best practice
3. Collaborative checking if necessary.
4. Education and Notification through collaboration among TLDs