SGNIC Registry Lock

By William Loh
SGNIC
Background

- Domain name hijacking is not uncommon. Number of incidents has been on the rise.
- Methods of hijacking includes: stolen credentials, social engineering, SQL injection attacks, or even the work of disgruntled employees.
Hijacking Examples

A number of high profile domain names have recently fallen victim to hijacking, including:

- NYTimes.com
- huffingtonpost.co.uk
- Washington Post
- Google.ps
- Linkedin.com
- Agence France-Press
- 60 Minutes
- CBS News
- Baidu
- BBC
Hijacking Consequences

- The impact of these hijacks can be significant.
- Hijackers can redirect emails and websites.
  - Loss of reputation and customer confidence
  - Loss of revenue
  - Loss of other credentials or sensitive information
An additional layer of security at the registry level which introduces the “human factor” to authorise changes.

Instead of the registry applying registrars’ request for changes automatically and immediately, each change needs to be communicated by an authorised entity directly to the registry.
Registry Deployments

Examples:

Verisign : .COM / .NET / .TV / .CC / .NAME
AFNIC : .FR
EURID : .EU
CIRA : CA
Nominet : .UK
CNNIC : .CN
HKIRC : .HK
AUDA: .AU
Verisign’s (.com .net, etc.) implementation:

- If an end customer requests a change to a Registry Locked domain, an authorized individual at the registrar must submit a request to Verisign to unlock the domain name.
- This requester is then contacted by Verisign via phone and required to provide an individual security phrase in order for the domain name to be unlocked.
- The requester needs to inform Verisign to re-lock the domain name after the change is completed.
- Registrars will usually charge between a few hundreds to a thousand dollars a year for registry lock service on each domain name.
SGNIC’s Implementation (proposed)

- System will allow submission of nameserver* changes by registrar but the changes will be “pending confirmation”.
- Domain Name Admin Contact will be notified (via email) to confirm the change.
- Admin Contact login to SGNIC portal via SingPass/SGNICID to confirm the change.
- SGNIC will applies the change once confirmation received.

* Contact updates, deletion, transfers etc. under study
SGNIC’s Implementation (proposed)

- Skip unlocking and locking steps.
- All changes are reviewed prior apply into the registry system will help to reduce unauthorised changes apply to the domain name.
- Near instant confirmation – no phone calling/verification processes
- 24 x 7 self-service – no need to adhere to registry’s and registrar’s working hours
- Free of charge encourage take up.

For registrars:
- No process / system changes
- Registrars can still act as admin contact to help registrant apply the change request.
Reference

- http://domainnamewire.com/2013/09/16/domain-name-registry-lock/
Thank You