Mobile DNS Validation
Strengthening Registry Services Security

March 24 2014

By Hasnul Hasan
Lesson Learnt

2013
MYNIC experiences 2 security incident of unauthorised DNS redirections.

July 2013
Hackers target MYNIC system and modify DNS information.

October 2013
Hackers target End-User account and modify DNS information.
Lesson Learnt

October Tragedy – What actually Happened

Hacker → July Attacks → MYNIC

End User Systems
Lesson Learnt

October Tragedy – What actually Happened

Hacker

Improved Security

MYNIC

End User Systems
Lesson Learnt

October Tragedy – What actually Happened

Hacker → October Attacks → End User Systems

Improved Security

MYNIC
Lesson Learnt

October Tragedy – What actually Happened

1. Hacker compromised the email account of the user.
2. Hacker went to MYNIC website to execute a password reset request for an account.
3. Email confirmation went out to the owner of the account for validation.
4. Since owner’s email account was compromised, the rest is history.
Lesson Learnt

What can we learn from the two incidents

1. End goal is always to modify DNS information. As MYNIC improves the security level of it’s own system, hackers find the weakest link by understanding the whole process.

2. Looking at just MYNIC own security is inadequate since expectations of end users and perceptions of the public is different
Lesson Learnt

What can we learn from the two incidents

3. There is no absolute security. We can make it harder to a point the investment is not worth the return.

4. Protection up to end user for the services given is becoming a necessity in order to mitigate as much as possible the risk of compromised in external systems.

Due to that MYNIC decided to introduce multi-factor authentication system to further mitigate the risk of unauthorized DNS modification.
What Multi Factor Authentication?

1\textsuperscript{st} Factor = What you \textbf{KNOW}  
(e.g. username & password)

2\textsuperscript{nd} Factor = What you \textbf{HAVE}  
(e.g. token, phone, smartcard, certificates)

3\textsuperscript{rd} Factor = What is \textbf{UNIQUE}  
(e.g. fingerprint, DNA, retina)

If one factor is compromised, other factors are still in placed to protect the user. MYNIC implements 2 Factor authentication (2FA).
2FA Types & Points of Protection

2FA Types

Deployment of myTAC 2-Factor (2FA) authentication modules.

**SMS** – *Computer authentication* with verification using **SMS**

**Smart** – *Smartphone* application-based (IOS & Android)

Points of Protection

– Authentication Process
– Password Recovery
– Request on sensitive transactions i.e. changing domain’s information
Smartphone Authentication Request
Smartphone Transaction Request

You have a name server IP change request for the following domain. Reject the request if you did not initiate the change from your .myNIC domain administration website.

**Request details:**
- **Date:** Wed, 31 Feb 2014
- **Time:** 2:00 PM
- **Domain:** .myNIC
- **Primary name server IPv4 address:** 100.100.100.100
- **Secondary name server IPv4 address:** 200.200.200.200
- **Primary name server IPv6 address:** 2001:0db8:1000:3::1
- **Secondary name server IPv6 address:** 2001:0db8:1000:3::3

Powered by a built-in YubiKey Nano technology.
Other Matters that are as important

• Pre-registration of mobile phone numbers

• Delegation capabilities for end users who outsource domain management

• Awareness exercise to users and additional support points for help desks

• Integration of the solution into the system
Thank you