



The best practice to protect your domain name

12 Dec 2016

Ben Lee

HKIRC

Copyright 2016 HKIRC. All rights reserved.





Security and .hk

- 🔒 HKIRC always strives to provide reliable, robust and secure services
- 🔒 maintaining customer confidence and trust is important for .hk
- 🔒 Customers are now more security-aware, and the demand for secure internet related services is growing








Is Domain Name being targeted?

- ✦ More attacks have been targeted on the Domain Name System (DNS)
- ✦ The potential threat and damage of DDoS attacks at the DNS are getting better known in Hong Kong



Why attack/protect DNS?

-  **Total Number of .hk is over 430,000**
-  **DNS** – Denial of services and data access
-  **Website defacement** – Loss of reputation / confidence
-  **E-commerce sites defacement / diversion** – Loss of business / confidence
-  **Email traffic diversion** – Confidential information leakage



DNS Ecosystem

#Registrant – to get a domain name for
Websites / Email services



#Registrar – to register and update
Name Server and IP address



#Registry – to register and provision a
Domain Name



#DNS Operator – to operate and
provision a Domain Name



Registration



Operation





Anycast DNS services

#Registrants #DNS Operators



Use or deploy anycast DNS services – enable larger amount of servers to handle DNS queries in multiple geographical locations



Protect DNS services against DDoS attacks



Involve cost - Make your decision by considering your risk level




Registry and Registrar Lock


#Registrants #Registrars

 **Enable Registry Lock and Registrar Lock** – a lock controlled by the Registry (or Registrar)


 **Protect against** unauthorized DNS changes

How it works:

 Registry (or Registrar) side “Locked” and prohibit NS and IP address records changes

 “Unlock” by authorised person with verification by Registry (or Registrar)

 a.k.a EPP server/client status



.hk Domain name monitoring service

#Registrants



- **Use a domain name monitoring service** - monitor the registration of .hk domain name(s) that is similar to your domain name





- **Detect malicious mimic** of your domain name or websites



- **Protect** the right of trademark holders



2-Factor authentication #Registrants #Registrars



-  **Enable 2-factor authentication** or Dual-Password
-  **Protect against** stolen password or guessing password to take over your domain names



DNSSEC

#Registrants #Registrars

#DNS Operators

-  **Enable DNSSEC** – DNS Security extension to add digital signatures for DNS data
-  **Detect** unauthorized change to DNS data



Enable Email authentication

#Registrants #DNS Operators



Enable Email authentication



Sender Policy Framework (SPF)



Domain Keys Identified Mail (DKIM)



Domain-based Message Authentication, Reporting & Conformance (DMARC)



Recipients can flag and/or **discard unauthenticated phishing or spam emails**



Protect against phishing or spam email using your domain name



Security management framework

#Registrars #DNS Operators



Setup Security management framework



- ✓ InfoSec policy
- ✓ Incident response / Business Continuity Plan and Drill
- ✓ Fast response to phishing and security incidents
- ✓ Hotline support
- ✓ Security audit



Increase readiness for managing new security risks



#All

-  **Security and Defense is an endless Cat and Mouse game**
-  **Stay alert for new security threats and vulnerabilities**



Thank you!

MyCity
My Domain

.hk