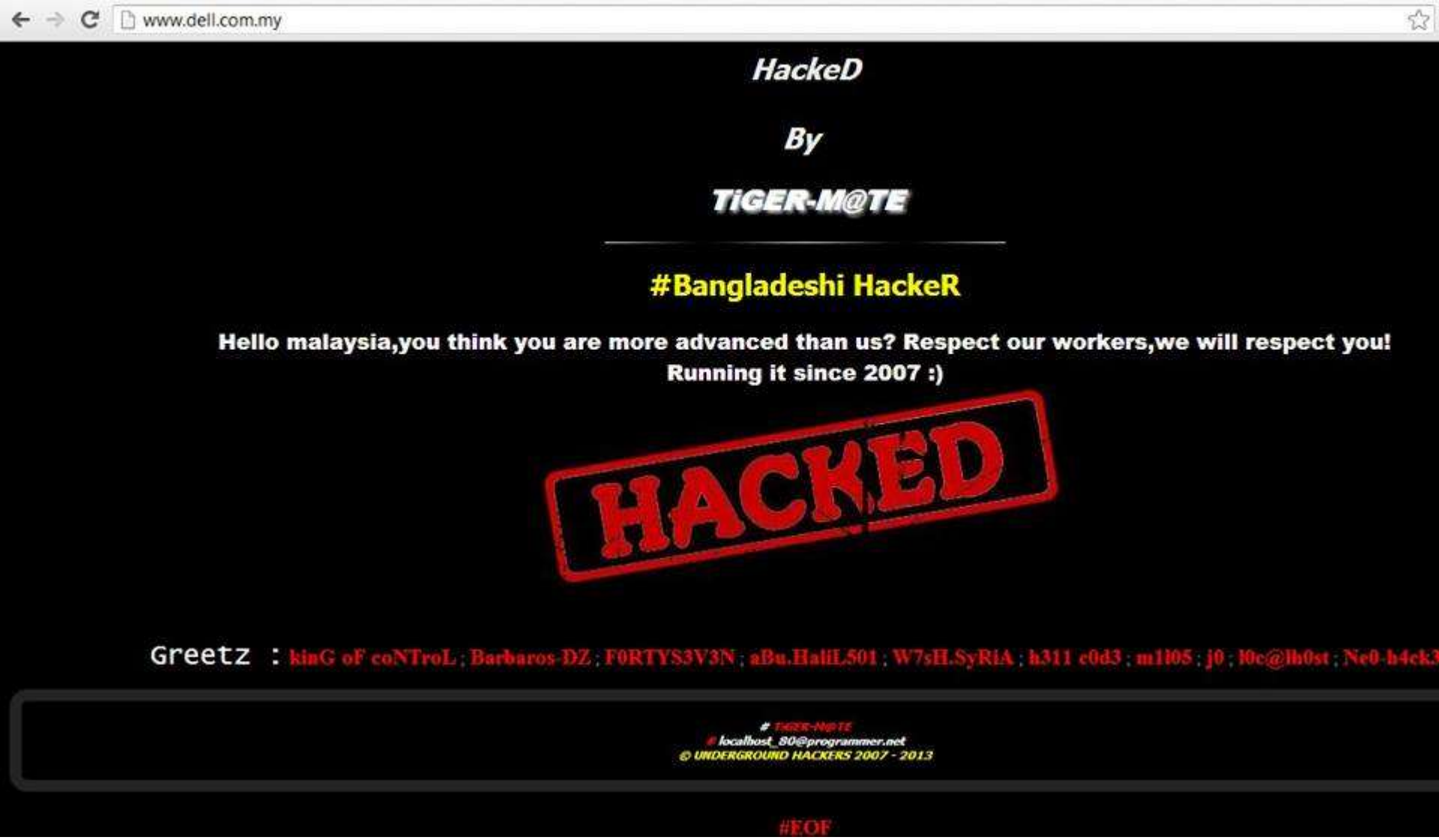
ccTLD incident

Matsuzaki ‘maz’ Yoshinobu
<maz@iij.ad.jp>

2013年7月1日

- マレーシアで不思議な事象
- 著名なwebサイトがいつもと違う
  - google, yahoo!, microsoft, kaspersky
  - dell, hp, coca-cola とかとか

http://www.dell.com.my/にアクセスしたら



http://www.digitalnewsasia.com/security/dns-poisoning-mynic-admits-servers-compromised

DNS?

- キャッシュポイズニングではないかという噂
  - http://plus.evozi.com/204/malaysia-domain-mynic-registry-hacked-numerous-my-sites-redirected/
  - ~~The quick fix for now would be to change your DNS servers either to your ISP's own DNS or to switch to OpenDNS. The list of available DNS servers are below.~~
- 何か良く分かってない"解決策"の流布

今日は外部から観測できた話のみ

;; AUTHORITY SECTION:

my.	172800	IN	NS	ns6.jaring.my.
my.	172800	IN	NS	dns.mynic.net.my.
my.	172800	IN	NS	dns2.mynic.net.my.
my.	172800	IN	NS	ns5.jaring.my.
my.	172800	IN	NS	**ns20.iij.ad.jp.**
my.	172800	IN	NS	ns-my.nic.fr.
my.	172800	IN	NS	ns2.cuhk.edu.hk.

一般にセカンダリDNSの機能

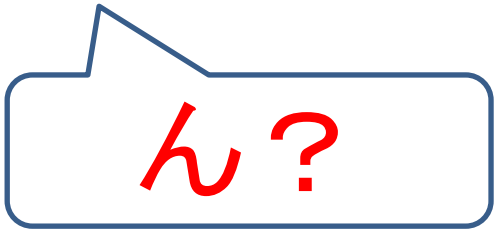
- 提供されたゾーンファイルをそのまま利用して応答する
  - 独自に変更したりしちゃいけない
  - 提供されたゾーンファイルこそが正しい
  - レジストリ情報との整合性は提供元で担保
- ちなみに、.myはDNSSEC署名済み
- .myの全てのDNSで同様の応答を返答中
  - 各DNSやゾーン転送がやられたわけじゃなさそう

whois

障害中

a [Domain Name] google.com.my
b [Registration No.] D1A145756
c [Record Created] 21-SEP-2010
d [Record Expired] 21-SEP-2013
e [Record Last Modified] 01-JUL-2013
:
k [Primary Name Server] SKEY0000029646
ns1.healthimpactnews.com 173.199.168.220

l [Secondary Name Server] SKEY0000029647
ns2.healthimpactnews.com 173.199.168.220



現在

a [Domain Name] google.com.my
b [Registration No.] D1A145756
c [Record Created] 21-SEP-2010
d [Record Expired] 21-SEP-2013
e [Record Last Modified] 01-JUL-2013
:
k [Primary Name Server] NS1GOOG0.SER
ns1.google.com 216.239.32.10

l [Secondary Name Server] NS2GOOG0.SER
ns2.google.com 216.239.34.10

どうもレジストリ情報が変

- やられたと言われているドメイン名のネームサーバが全て特定のホストに向いている
- でもって、そのDNSにwww.ドメイン名を問い合わせると同一のIPアドレスを応答
  - アクセスすると冒頭のwebサイトに誘導
  - ちなみに、malwareのダウンロードなどは行われていなかった模様

MyNICからのレポート1

- http://mynic.my/en/news.php

Dear Valued Customers,

We are regret to inform you that we have today discovered some problems with our system which had resulted in an unauthorised change in some of the domain name’s servers information without the permission of original registrant (owner of domain name). This may lead to website redirection as experienced in a few reported cases.

MYNICからのレポート2

.my DOMAIN NAME INCIDENT RESOLVED

SERI KEMBANGAN, Selangor, 2nd July 2013 – MYNIC has resolved the .my domain name incident which resulted in an unauthorised change in some of the domain name's servers information without the permission of the original registrant (owner of domain name).

The problem, which affected several .com.my and .my domain names, has led to website redirection as experienced in a few reported cases yesterday. However the affected domain name information has been successfully restored on the same day.

まとめ

- レジストリ情報が狙われた
  - DNS的には正常なDNSエントリの更新
  - DNSSEC的にもとっても正しい
- レジストリ、レジストラは登録者の情報を守るため、あれこれ頑張ってほしいね