Un peu de story telling, pour commencer

- `http://linuxfr.org/users/gaetan_63/journaux/histoire-d-un-vol-de-domaine`, 15 mai 2015
- Un projet de logiciel libre avec son nom de domaine, pas tellement géré (pas de responsable clair, une attitude de « on verra quand on en aura besoin »)
- Le nom expire et est repris par un domaineur (les gens qui achètent et vendent des noms)
- Il veut bien le revendre, mais pour 400 $
- Un incident possible, parmi tous ceux qui peuvent frapper les noms de domaine

Avant l'incident

- Tout l'Internet repose sur le DNS
- Ce n'est pas une simple application, c'est un élément de l'**infrastructure** (comme BGP)
- Indispensable et souvent oublié
- La perte d'un nom peut être irréparable

Un écosystème compliqué

Le monde des noms de domaine est difficile pour la sécurité, en raison de sa complexité et de la profusion d'acteurs

- Pour la **résolution** de noms, la racine, le TLD, votre hébergeur DNS...
- Pour l'**avitaillement**, le registre, le BE (Bureau d'Enregistrement, *registrar* en états-unien), parfois un revendeur...

Précautions

- Surtout, gardez à jour la liste des contacts, et leurs coordonnées
- Les contacts doivent être responsables (par exemple, ils doivent lire leur courrier)
- Mettez bien les mots de passe sur un post-it affiché à la cantine
- Veillez au nombre et à la diversité des serveurs
- Logiciels sérieux et mis à jour
- Bien choisir ses partenaires et testez les (et attention à la loi dont ils dépendent)
- Ne pas croire que les *firewalls* protègent

Un de ces conseils est faux. Lequel ?

Précautions, suite

- Sensibilisez tout le monde à l'**ingéniérie sociale** et au *spear phishing*.
- Vérifiez la supervision technique : êtes-vous bien prévenu si un serveur défaille ?

L'incident

Des menaces très variées...

- Le Ministère de la Culture et de la Communication oublie de renouveller son nom de domaine, qui est suspendu
- TLD `.my` plusieurs fois piraté (la dernière fois au printemps 2015)
- Août 2013, la SEA prend le contrôle du nom de domaine du New York Times
- Janvier 2015, « Attaque » « Poivre du Sichuan » depuis la Chine, utilisant le DNS comme redirecteur
- Printemps 2015, Attaque « *random qnames* » contre beaucoup de domaines (dont `.wf` et `.pt`)

Classement des attaques

- Perte ou détournement du nom
- Déni de service

Réponses

- (Détournement) Surtout, attention aux caches : une fausse manœuvre peut les empoisonner pendant des heures, voire des jours
- (Détournement) Ne pas annoncer quoi que ce soit avant d'être sûr de la réparation
- (DoS) Débrancher le *firewall*, qui a en général foutu le souk
- (DoS) Analyser l'attaque et développer des contre-mesures (suggestion : Netfilter est génial et fait presque le café) **La réaction aux DoS nécessite compétences et réactivité.**
- (Tous les cas) Stocker les faits, car ils ne durent pas. `dig @8.8.8.8 mondomaine.example`, `whois mondomaine.example`

Bibliographie

- Dossier thématique AFNIC n° 9 « Sécuriser la gestion des noms de domaine » `https://www.afnic.fr/fr/ressources/publications/dossiers-thematiques/securiser-la-gestion-des-noms-de-domaine.html`
- Journée du Conseil Scientifique de l'AFNIC (JCSA) en juillet 2012 « Sécurité des noms de domaine »
- ANSSI « Bonnes pratiques pour l'acquisition et l'exploitation de noms de domaine » `http://www.ssi.gouv.fr/guide/bonnes-pratiques-pour-lacquisition-et-lexploitation-de-noms`