Probables attaques à venir

Quelles cibles ?

Tout est cible potentielle (*cf. générique CSICyber)* :

- données personnelles (cf. Ashley Madison) ;
- l'activité économique (espionnage, sabotage, subversion) ;
- la recherche (cf. vidéo Blacklist) ;
- l'information (SEA et attaque Maison Blanche).

Mais aussi les matériels (proximité de navires russes près des câbles sous-marins).

Sans oublier les logiciels (altérés).

Quels auteurs ?

Les amateurs :

- joueurs ;
- la voie professionnalisante.

Les ennemis (déclarés, mercenaires → ANSSI).

Les hacktivistes :

- Anonymous ;
- cyber armées ;
- collectifs en tout genre.

Les concurrents.

Les groupes maffieux (toute criminalité).

Quels moyens ?

Web classique :

- packs de maliciels téléchargeables ;
- ingénierie sociale sur mesure ;
- vol de *solutions* de cybersécurité offensive (Gamma international 2014 *Finfisher*, Hacking Team 2015 *RCS*) ;
- l'information (SEA et attaque Maison Blanche).

Les réseaux sociaux (*News online newscaster*).

Quels moyens ?

L'internet des objets :

- télé-santé (pacemakers *Homeland*, pompes à insuline *Person of Interest*) ;
- véhicules connectés ;
- altération de preuves numériques ;

Big Data (cf. vidéo Satisfaction).

Quelles caractéristiques ?

Plus grande sophistication des attaques, effectuées sur mesure (Stuxnet, vidéo MmSecretary).

Location de « pirates à gage » ce qui permet de masquer la source de l'attaque.

Plus grande fréquence des attaques (ANSSI).

Risque d'attaques disséminées pour créer de la saturation (idem attaques terroristes).

Le temps travaille pour l'attaquant (ANSSI).

Quels remèdes ?

Classification de l'information.

Protéger l'information (cf. vidéo Homeland).

Prise de conscience des dirigeants (ANSSI).

Le plus gros problème n'est pas technique mais organisationnel.

Se souvenir du procès de l'Aquila.

Débat