

Approche technique de l'espace numérique

Chapitre 4

Qu'est ce qu'une cyberattaque ?



Pablo Rauzy <pr@up8.edu>
pablo.rauzy.name/teaching/aten

Qu'est ce qu'une cyberattaque ?

- ▶ On appelle *cyberattaque* toute offensive menée à travers un dispositif informatique.

- ▶ On appelle *cyberattaque* toute offensive menée à travers un dispositif informatique.
- ▶ Cette définition est *très* large et peu informative.
- ▶ Essayons d'y voir plus clair à travers une classification des différents types d'attaques.

- ▶ Au fur et à mesure de la construction de notre classification, on va discuter des exemples, plus ou moins précis, de types d'attaque.
- ▶ Essayez systématiquement de vous questionner sur la pertinence de l'appellation "cyber".

- ▶ Selon quels critères établir une classification ?

- ▶ Selon quels critères établir une classification ?
 - Par techniques ?
 - Par objectifs ?
 - Par acteurs ?
 - Par ampleurs ?

- Là aussi, il y a plusieurs façons “hauts niveaux” raisonnables de classer les attaques :
- passives ou actives,
 - réseaux ou internes,
 - syntaxiques ou sémantiques,
 - volatiles ou persistantes,
 - exploitation de failles techniques ou humaines,
 - ...

Attaques passives ou actives

- ▶ Une attaque est *passive* si elle consiste seulement en de l'écoute.
 - Exemples : écoutes téléphoniques, captures de trafic réseau, scan de ports.
- ▶ Une attaque est *active* si elle nécessite d'agir sur un système.
 - L'intervention sur le système peut être invasive ou non, destructive ou non.
 - Exemple : attaque de l'intercepteur en cryptographie.

Attaques invasives ou non

- ▶ Une attaque active est *invasive* si elle nécessite une intrusion sur un système.
 - Exemple : dépassement de mémoire tampon.
- ▶ Autrement, elle est non invasive.
 - Exemple : déni de service.

Attaques destructives ou non

- ▶ Une attaque active est *destructive* si elle casse un système ou supprime de l'information.
 - Exemple : ransomware.
- ▶ Autrement, elle est non destructive :
 - Exemple : spyware.

Attaques réseaux ou internes

- ▶ Une attaque qui nécessite de s'être introduit sur le système cible est *interne*.
 - Exemple : élévation de privilèges.
- ▶ Autrement l'attaque peut être menée à travers le réseau.
 - Exemple : routage BGP (Internet), usurpation d'IP (réseau local).
- ▶ Selon la nature du système cible, pas évident de distinguer l'une de l'autre.
 - Exemple : attaque sur le réseau interne d'une entreprise.

Attaques syntaxiques ou sémantiques

- ▶ Nomenclature très informaticienne...
- ▶ Une attaque est *sémantique* si sa méthode est la dissémination de fausses informations.
 - Exemple : armée de bots sur les réseaux sociaux, publicités.
- ▶ Dans les autres cas, l'attaque est *syntaxique*.

Attaques volatiles ou persistantes

- ▶ Une attaque est *persistante* si elle permet de se maintenir dans le système cible.
 - Exemple : virus installant un client pour un botnet.
- ▶ Une attaque est *volatile* dans le cas contraire.
 - Exemple : un déni de service s'arrête rapidement lorsque l'attaque cesse.

Attaques exploitant des failles techniques ou humaines

- ▶ La plupart des attaques réelles utilisent les deux à différentes étapes.
- ▶ On appelle souvent l'exploitation de failles humaines *ingénierie sociale*.
 - Exemple : se faire aider à entrer dans un bâtiment protégé.
- ▶ Les attaques techniques exploitent des *vulnérabilités*.
 - Exemple : CVE, 0day, exploits, canaux auxiliaires, ...

Classification par objectifs

- ▶ Le recours à une cyberattaque peut avoir de nombreux objectifs.
- ▶ L'objectif peut être direct ou indirect, si il sert à la mise en place d'attaques ultérieures.

Classification par objectifs

- ▶ Le recours à une cyberattaque peut avoir de nombreux objectifs.
- ▶ L'objectif peut être direct ou indirect, si il sert à la mise en place d'attaques ultérieures.
- ▶ Exemple d'objectifs indirects :
 - récupérations d'adresses emails pour pourriel ou hameçonnage,
 - infiltration d'un réseau interne,
 - constitution d'un botnet.
- ▶ Exemple d'objectifs directs :
 - récupération massive de moyens de paiement ou de données personnelles à revendre,
 - attaque sur un site web politique (hacktivism),
 - espionnage (dont OSINT, SIGINT),
 - cyberguerre.

Classification par acteurs

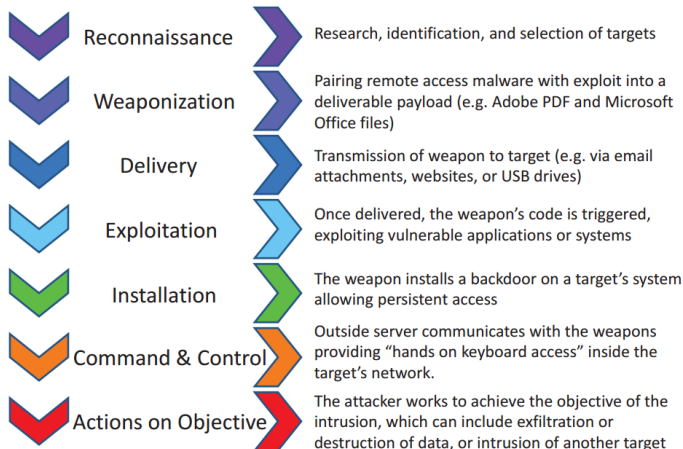
- ▶ Une cyberattaque peut être menée par un individu seul aussi bien que par un état.
- ▶ Il y a évidemment tout un spectre possible entre les deux :
 - criminels,
 - groupes d'hacktivists (L0pht, CCC, cDc, Anonymous, LulzSec, ...),
 - entreprises,
 - agences de renseignements,
 - ...

Classification par ampleurs

- ▶ Il peut aussi être pertinent de classer les attaques par leur ampleur.
- ▶ Là aussi, il y a tout un spectre possible :
 - attaquer le wifi de son voisin pour utiliser sa connexion ou usurper son identité,
 - faire tomber un site web politique,
 - récupérer les données de paiement d'une grande chaîne de magasins ou d'un store en ligne,
 - compromettre le réseau d'un hôpital,
 - espionner le trafic Internet d'un pays,
 - attaquer des centrales nucléaires.
- ▶ Évidemment, l'ampleur est liée à l'acteur.

Déroulement d'une attaque

- ▶ Une vision standardisée du déroulement d'une attaque a été proposé en 2011.
- ▶ On l'appelle généralement la "cyber kill chain".



source : wikimedia commons, domaine public.