Approche technique de l'espace numérique

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

UNIVERSITÉ PARIS 8 VINCENNES-SAINT-DENIS
Institut Français de Géopolitique / M2 Cyberstratégie & Datascience

Séance 1

Qu'est ce qu'une cyberattaque ?
Étude de cas : Stuxnet

Qu’est ce qu’une cyberattaque ?

Cyberattaque

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

Cyberattaque

- 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".

Classification des attaques

- Selon quels critères établir une classification ?

Classification des attaques

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

Classification par techniques

- 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'homme du milieu 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

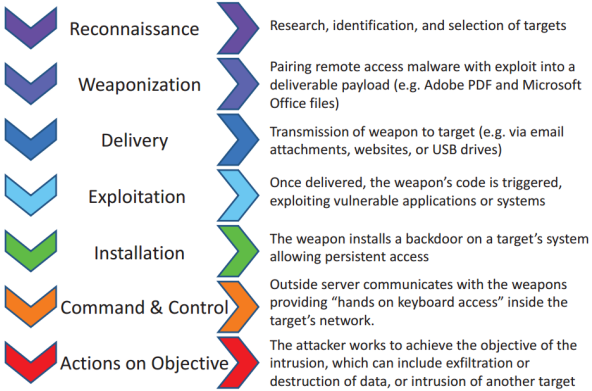
- Une cyberattaque peut être menée par un individu seul aussi bien que par un état.
- Il y a évidemment tout un spectre possible entre les deux :
  - criminels,
  - groupes d'hacktivists (L0pht, CCC, cDc, Anonymous, LulzSec, ...),
  - entreprises,
  - agences de renseignements,
  - ...

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.

Étude de cas : Stuxnet

Présentation

- Stuxnet est un *ver* informatique pour le système Windows.
- Il a été découvert en 2010 par une société de sécurité informatique biélorusse.
- Il ciblait centrifugeuses iraniennes d'enrichissement d'uranium.
- Il aurait contaminé 45000 systèmes dont 30000 en Iran.
- Il s'agirait de la première *cyber arme* conçue pour attaquer un système industriel précis.

- Un *ver* est un logiciel malveillant capable de se propager à travers un réseau informatique.
- Au contraire d'un virus il n'a pas besoin d'un programme "hôte" (autre que le système).

Mode opératoire

- Stuxnet procède en 3 étapes :
  - Infecter des Windows jusqu'à en trouver qui contiennent les logiciels Siemens PCS 7.
  - Infecter le logiciel Step 7 (interface utilisateur du *SCADA* visé).
  - Infecter les machines Siemens S7 PLC contrôlées par ce logiciel.

- Acronyme de “Supervisory Control And Data Acquisition”.
- Système de gestion qui prend des décisions en temps-réel en fonction de mesures.

Étape 1 : Windows

- Stuxnet s'introduit sur les réseaux internes et saute les *air gap* par clef USB.
- Il s'installe sur les systèmes Windows grâce à un *0day* (CPLINK).
- Il se diffuse à travers le réseau en utilisant différents *exploits* et 0days (partage d'imprimantes, LNK/PIF, ...).
- Il contient deux *rootkits* un au niveau utilisateur et un au niveau noyau.
- Il contient un *pilote* qui a été *signé* par des certificats volés à JMicron et Realtek (deux entrepries sur le même campus à Taiwan).
- Deux sites web lui servent de *C&C* (au Danemark et en Malaisie).
- Il est très gros pour un malware (un demi mégaoctet), et programmé en plusieurs *langages* (notamment C et C++).

- On parle d'*air gap* quand un système ou un réseau est physiquement déconnecté de tout autre réseau.
- D'où la nécessité d'utiliser une attaque via clef USB pour y pénétrer.
- Stuxnet était donc prévu pour attaquer un réseau sensible.

- Un *0day* est une vulnérabilité qui n'a jamais été divulguée.
- Son utilisation dans un malware le révèle le plus souvent quand celui-ci est analysé.
- Stuxnet exploite quatre 0day différents, ce qui est complètement inhabituel.

- Un *exploit* est un composant d'un programme permettant d'exploiter une vulnérabilité.
- Il peut s'agir d'un exploit distant pour se connecter à un autre système, ou d'un exploit local pour accéder à des privilèges supérieurs par exemple.
- Stuxnet utilise plusieurs exploits réseaux et locaux.

- Un *rootkit* est un ensemble de technique visant à pérenniser et cacher la présence d'un malware dans un système.
- Ce sont des logiciels assez complexes.
- Ce n'est jamais utilisé avec de bonnes intentions.
- Stuxnet en utilise plusieurs à différents niveaux et sur différents types de système.

- Programme dont le rôle est de permettre l'interaction entre un logiciel et un périphérique.
- Quand un pilote doit s'installer dans un système critique, il est parfois requis que celui-ci soit signé.
- Stuxnet embarque un pilote pour intercepter et altérer les communications entre le logiciel de contrôle et supervision des centrifugeuses et ces dernières.

- Une *signature* est un garantie cryptographique de l'authenticité et de l'intégrité d'une donnée (qui peut-être un logiciel).
- Cela suppose l'utilisation de cryptographie asymétrique, c'est à dire une clef privée qui permet de faire la signature et une clef publique qui permet de la vérifier.
- Stuxnet embarque deux signatures valides par deux entreprises différentes pour son pilote, ce qui signifie que les clefs privées ont été volées.

- *C&C* est l'abréviation de "*command and control*".
- C'est comme ça qu'on désigne le serveur maître d'un parc de systèmes infestés par un rootkit.
- Il peut servir à contrôler un botnet, ou à collecter des informations, par exemple.
- Stuxnet utilisait un C&C pour être mis à jour et pour de l'espionnage industriel.

- On parle ici de *langage de programmation*.
- La plupart des malwares n'en utilisent qu'un seul.
- Stuxnet utilise plusieurs langages, ce qui peut laisser penser qu'il a été développé par plusieurs équipes.

Étape 2 : Step 7

- Une fois sur un Windows, Stuxnet infecte les fichiers des logiciels WinCC et PCS 7.
- Il utilise entre autre un 0day pour accéder à la *base de données* du logiciel.
- Il peut alors modifier la configuration du logiciel.
- Il subvertie la *bibliothèque* "`s7otbxdx.dll`" qui sert à la communication entre WinCC et les Siemens S7 PLC.
- Il peut alors intercepter les communications et les altérer de manière masquée.
- Ça lui permet de s'installer sur les PLC de manière invisible, et de masquer sa présence.

Base de données

- Une *base de données* est littéralement ce que ça décrit.
- Stuxnet utilise un 0day qui lui permet de lire et d'écrire dans la base de données de Step 7 (un mot de passe écrit en dur dans le code, ce qui laisse penser que le logiciel coopère).

- Une *bibliothèque* (ou *librairie* par anglicisme) est un ensemble de composants qu'on utilise dans un ou plusieurs logiciels et qui peut être développé séparément de ceux-ci.
- Stuxnet modifie la bibliothèque qui s'occupe de la communication avec les centrifugeuse, pour faire une attaque de l'homme-du-milieu.

Étape 3 : Siemens S7 PLC

- Étape moins connue par le code n'a pas été publié.
- Visiblement le malware n'agit pas sauf si il reconnaît une configuration précise.
- Quand il agit, il modifie périodiquement la vitesse de rotation des moteurs du système.
- Il installe également un rootkit pour se rendre invisible.