Cyberguerre et cyberdéfense

23.03.2015
Gérard Peliks
LTC Réserve Citoyenne de Cyberdéfense DGGN
gerard.peliks@noos.fr
Expert Sécurité

Cyberguerre et cyberdéfense

- **Les dangers du cyberespace**
- Des attaques sur les organisations
- Vivre avec les menaces, mais réagir

Quelle est la durée de vie de votre PC non protégé ?

- Durée de vie d'un PC sous Windows, directement connecté à l'internet, sans antivirus à jour, ni firewall personnel

En 2003 : 40 minutes
En 2004 : 20 minutes

Selon le SANS Institute
www.sans.org

Aujourd'hui : 3 minutes

Exemples de pertes dues aux attaques

- Coût moyen suite à une cyberattaque, en 2014, en France ?

  561 000 €

  En 2013, 280 000 € (+200% d'augmentation)

  Source : FIDAL

- Coût d'une panne majeure des systèmes d'information en Europe ?

  250 milliards de dollars
  Source : CSI COMPUTER SECURITY INSTITUTE

  Une telle panne a une probabilité de 10 à 20% de se produire dans les 10 prochaines années
  Imaginez : Plus d'électricité, plus de transports…

- Coût mondial estimé du cybercrime en 2014 ?

  Environ 600 milliards de dollars

  Source : *Forum international sur la communication commerciale*
  Sept. 2014

Attaques sur les 3 couches du cyberespace

Couche de la signification

Couche des logiciels

Couche des infrastructures

La disponibilité de l'Information tient parfois à un fil…

Source : ITespresso.fr

Vélizy, mai 2011

Source : ITespresso.fr

matelsom : 250.000 euros de perte, 120 personnes au chômage technique

Attaques sur les 3 couches du cyberespace

Couche de la signification

Couche des logiciels

Couche des infrastructures

Failles d'aujourd'hui : Heartbleed

Le 08 Avril 2014

Des chercheurs alertent sur une faille critique dans OpenSSL

La menace Heartbleed touche plusieurs versions d'OpenSSL

Les experts en sécurité informatique conseillent aux administrateurs de corriger une faille critique dans OpenSSL, une librairie Open Source de protocoles de chiffrement qui est utilisé par un grand nombre de sites web.

Plusieurs spécialistes de la sécurité ont alerté les administrateurs des sites web afin qu'ils corrigent une faille importante dans OpenSSL. Cette vulnérabilité est surnommée « Heartbleed » et se trouve dans plusieurs versions d'OpenSSL, une bibbliothèque Open Source de chiffrement pour communiquer en SSL (Secure Socket Layer) ou TLS (Transport Security Layer). La plupart des sites utilise ce système de chiffrement caractérisé par la présence dans les navigateurs du symbole du cadenas. La faille a été découverte en décembre 2011, mais elle vient d'être corrigée par la version 1.0.1g d'OpenSSL publiée hier. Selon **un site spécialement mis en place**

Attaques sur les 3 couches du cyberespace

Couche de la signification

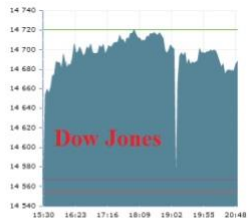
Couche des logiciels

Couche des infrastructures

Un répertoire de Web défacés : www.zone-h.org/archive

Plus de xxxx Webs, en France défigurés du 7 au 9 janvier 2015

Faux tweet sur Associated Press (23 avril 2013)



http://sea.sy/

le Dow Jones (DJIA) perd 145 points

136 milliards de dollars de pertes sur l'indice boursier !!!

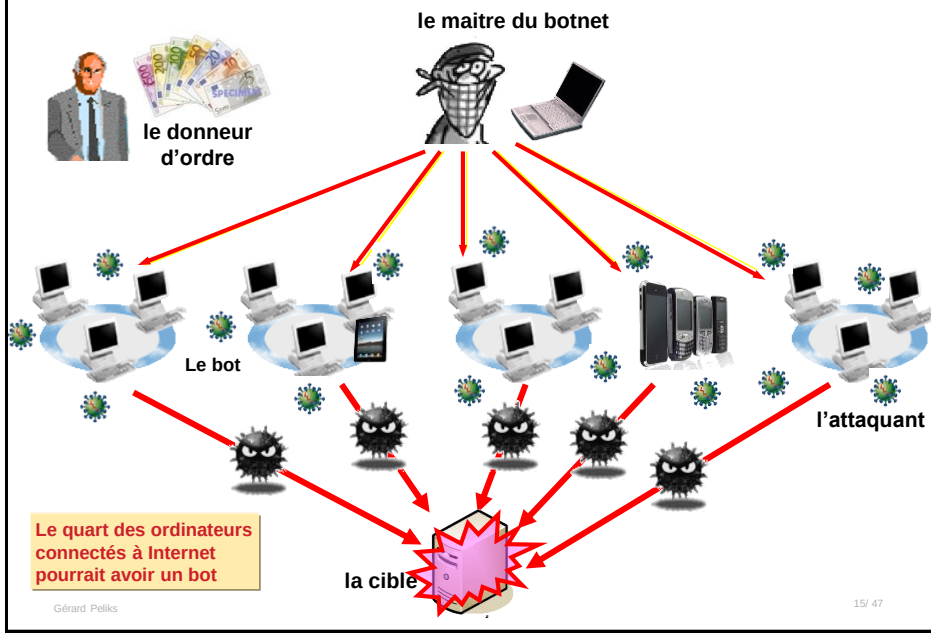
Cyberguerre et cyberdéfense

- Les dangers du cyberespace
- **Des attaques sur les organisations**
- Vivre avec les menaces, mais réagir

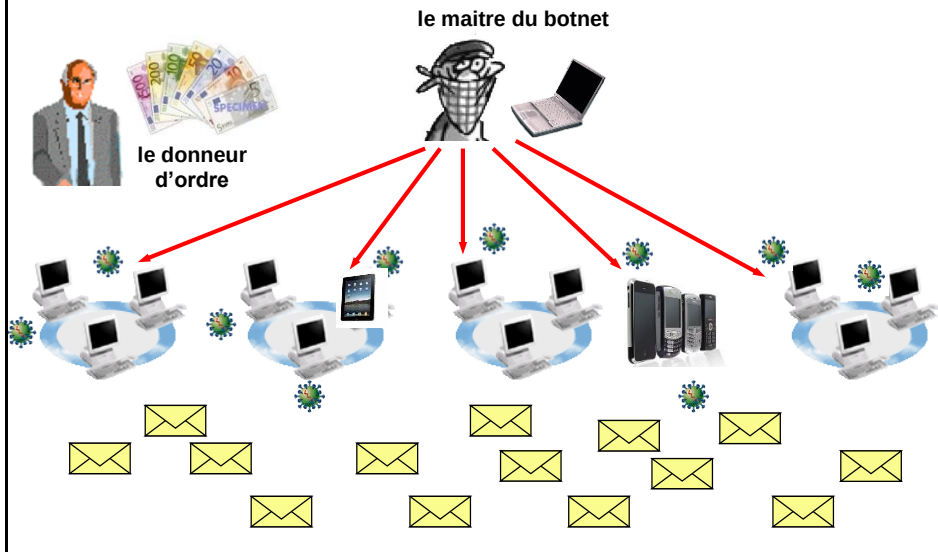
Les attaques notables sur les organisations entre 2007 et 2011

- Estonie 2007 : **Les botnets**
- Iran 2010 : Le ver Stuxnet : Les SCADA
- Bercy, Areva, Sony 2011 : Les APT

Le botnet : attaques en dénis de services distribués



Le botnet pour spammer



Les attaques notables sur les organisations entre 2007 et 2011

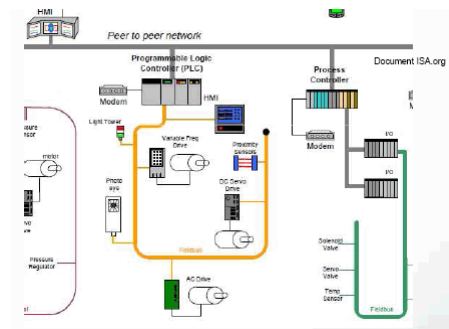
Estonie 2007 : Les botnets

Iran 2010 : Le ver Stuxnet : **Les SCADA**

Bercy, Areva, Sony 2011 : Les APT

Stuxnet : Attaques sur les SCADA (*)

Stuxnet



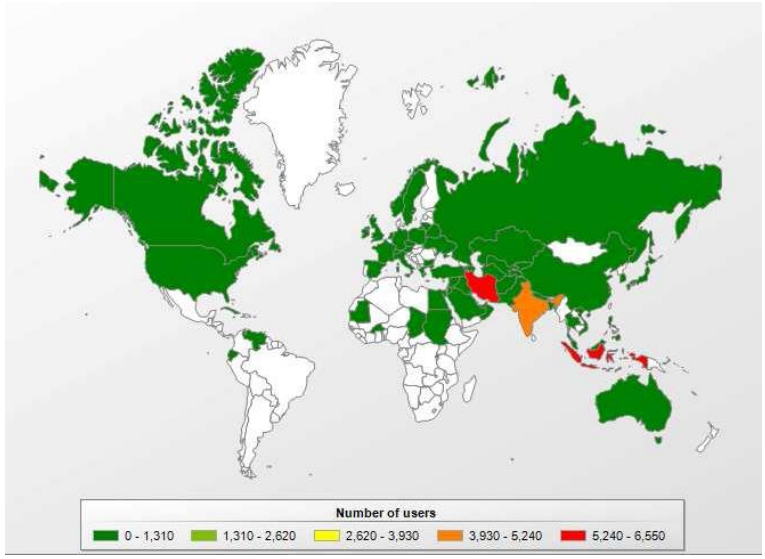
(*) **Supervisory Control And Data Acquisition**

Le ver Stuxnet : Les attaques sur les SCADA

Une coopération USA / Israël (programme Olympic Games)

- 10 000 heures-hommes de développement
- 4000 fonctions différentes
- Exploitation de 4 "zero-day attacks" (= attaques sur des vulnérabilités inconnues)
- Logiciels signés par usurpation (les USA peuvent le faire...)
- Une erreur dans le sabotage : 100 000 ordinateurs infectés dans le monde

Stuxnet, se répand hors de l'Iran



Stuxnet … arrive en France

HACKER OUVERT

LA SOCIÉTÉ AIR LIQUIDE PIRATÉE PAR STUXNET

Le géant français des gaz industriels a été victime du célèbre virus créé pour viser le programme nucléaire iranien.

Shodan, le moteur de recherche pour objets et systèmes connectés

https://www.shodan.io/

Les attaques notables sur les organisations entre 2007 et 2011

Estonie 2007 : Les botnets

Iran 2010 : Le ver Stuxnet : Les SCADA

Bercy, Areva, Sony 2011 : **Les APT**

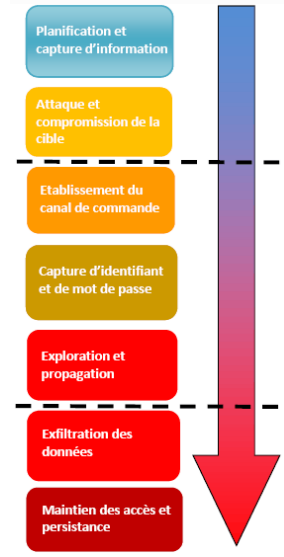
Les attaques par APT
(advanced persistent threats)

Les APT, 1/3 de marketing sécurité, 1/3 de gros titres dans la presse, 1/3 de petits mensonges ?

NON !

Une APT est une attaque ciblée qui agit silencieusement et s'installe dans le système d'information cible, avec pour objectif de collecter et corrompre des informations sensibles sur le long terme, plutôt que de réaliser un gain immédiat.

Une APT toutes les 1,5 secondes !



Quelques chiffres de perte suite à des attaques APT

- Areva :
  - plusieurs millions d'euros pour reconstruire le réseau ?
  - préjudice économique résultant du vol des informations ?
- Sony :
  - plusieurs centaines de millions de dollars ?
- ……

Cyberguérilla, cybercombat de rue ou cyberguerre ? 2012…

Flame : Le **cyber espionnage** massif

Elysée : L'exfiltration et la destruction de données

Shamoon : La destruction du système de gestion

Flame écoute vos conversations

L'Iran et d'autres pays du Moyen Orient contaminés

- Flame arrive avec une mise à jour de Windows
- C'est un logiciel espion, avec key logger et screen saver
- Il écoute les conversations des smartphones à proximité, par Bluetooth
- Il porte une boite à outils de 20 Mo
- Il est écrit en un langage peu connu : Lua
- Il s'autodétruit sur commande à distance

Cyberguérilla, cybercombat de rue ou cyberguerre ? 2012…

Flame : Le cyber espionnage massif

Elysée : **Exfiltration et destruction** de données 

Shamoon : La destruction du système de gestion

Gardez moi de mes amis, je m'occupe de mes ennemis…

Source : Lexpress 20//11/2012

Cyberguérilla, cybercombat de rue ou cyberguerre ? 2012…

Flame : Le cyber espionnage massif

Elysée : **Exfiltration et destruction** de données

Rapport Bockel

ANSSI

LIVRE BLANC SUR LA DEFENSE ET LA SECURITE NATIONALE

PROJET DE LOI DE PROGRAMMATION MILITAIRE 2014 / 2019

LPM

Réserve Citoyenne de Cyberdéfense

Shamoon : La destruction du système de gestion

Cyberguérilla, cybercombat de rue ou cyberguerre ? 2012…

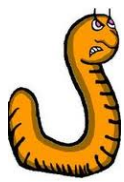
Flame : Le cyber espionnage massif

Elysée : Exfiltration et destruction de données

Shamoon : La **destruction du système** de gestion

Shamoon, la réponse de l'Iran

- Une attaque destructrice
- 30 000 ordinateurs détruits en octobre 2012
- 2 semaines pour rétablir les services informatiques
- Les installations gazières du Qatar aussi touchées



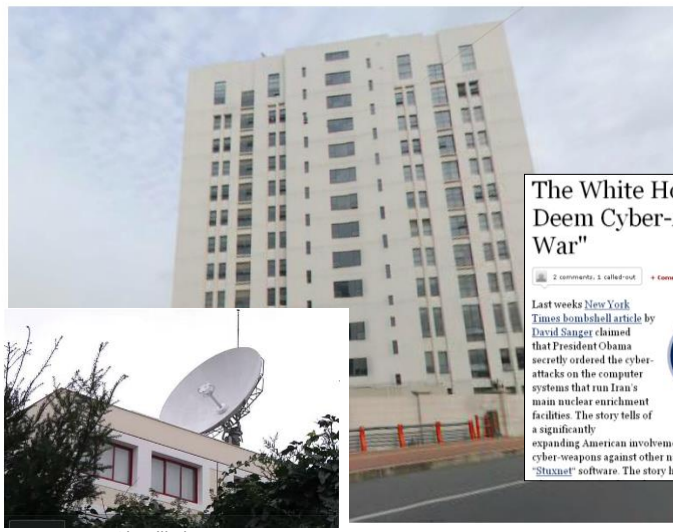
Source : TradeArabia

2013, l'année du cyber espionnage

APT1 : Le rapport Mandiant accuse la Chine

PRISM : L'espionnage par les Américains

APT1 : L'espionnage par les Chinois



Chevilly-la-Rue

Shanghai, Unité 61398

Source : Datanews

Source : Forbes

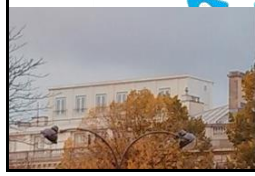
2013, l'année du cyber espionnage

- APT1 : L'espionnage par les Chinois

- Prism : L'espionnage **par les Américains**

PRISM : L'espionnage par les Américains

Source : 01net



Source : Gizmodo

2014, vols d'identités numériques et grosses failles décelées

- Vols de données à caractère personnel
  - Target — Vol de données de 110 millions de clients
  - Orange — avril : 1.3 millions de e-mails clients et prospects volées
  - Cybervor — 1,2 milliards de login / mots de passe hackés par des russes
  - JP Morgan — octobre : 80 millions de comptes utilisateurs
- Grosses failles décelées
  - Heart Bleed
  - Shell Shock

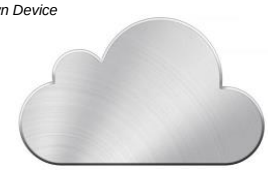
Vos fichiers chiffrés par bitlocker

Cyberguerre et cyberdéfense

- Les dangers du cyberespace
- Des attaques sur les organisations
- **Vivre avec les menaces, mais réagir**

Demain, entre la paranoïa et la naïveté, l'heure est aux sueurs froides…

- Smartphones, tablettes, BYOD ? *Bring Your Own Device*
- Cloud Computing ?
- HaaS ?
- APT ? *Advanced Persistent Threats*
- SCADA ? *Supervisory Control and Data Acquisition*
- Big Data ?
- Objets communicants ?
- Monnaies virtuelles
- HFT
- ……..



… et l'heure est à la cybersécurité

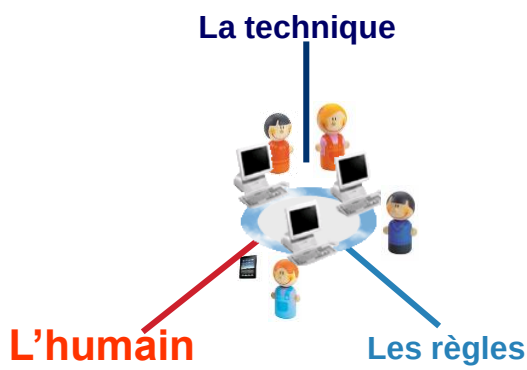
La sécurité des systèmes d'information

Qu'est ce que la sécurité de l'information ?

Ensemble des mesures techniques et non techniques de protection permettant à un système d'information de résister à des évènements susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles.

www.ssi.gouv.fr

L'humain au centre de la sécurité



L’humain au centre de la sécurité

Source : Hapsis

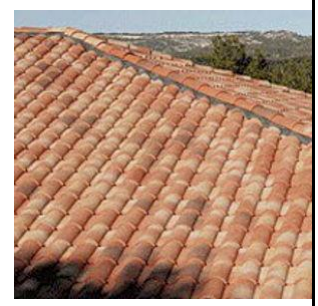
Plate-forme PHAROS de l‘OCLCTIC : www.internet-signalement.gouv.fr/

130 000 signalements par an, 400 par jour

38 000 signalements,entre le 7 et le 30 janvier 2015

Les tuiles qui protègent de la pluie ont toutes été posées par beau temps

用瓦盖 *Proverbe chinois*



Merci pour votre attention!

Des questions?

Gérard Peliks
gerard.peliks@noos.fr