UE - Sécurité

Généralités

Jean-Marc MULLER
Sébastien SCHMITT

Sommaire

- Les enjeux de la sécurité informatique
- La cybercriminalité
- Attaques de grandes ampleurs
- Panorama des menaces
- Aspect juridique de la sécurité des SI

QUESTION

Qu'est ce que la notion de : (CYBER) SECURITE ?

Les enjeux de la sécurité informatique

- Les enjeux fondamentaux pour les SI (Systèmes d'informations)

  - La sécurité a pour objectif de **réduire les risques** pesant sur le système d'information, pour **limiter leurs impacts** sur le fonctionnement et les activités métiers des organisations…

  - La gestion de la sécurité n'a pas pour objectif de faire de l'obstruction. Au contraire :

    - **Contribuer** à la qualité de service de l'infrastructure

    - **Garantir** la protection des données professionnelles

    - **Garantir** la protection des données personnelles

Les enjeux de la sécurité des SI

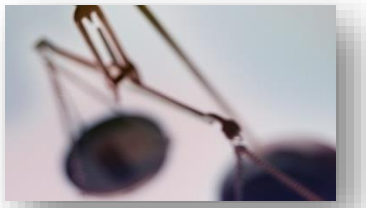
- Les enjeux stratégiques

Impacts financiers

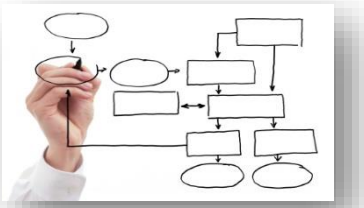
Impacts sur l'image et la réputation

Sécurité des S.I.

Impacts juridiques et réglementaires



Impacts organisationnels



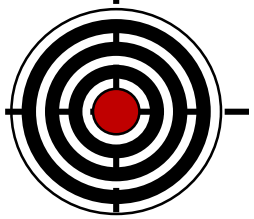
Source : Cyberedu

Les enjeux de la sécurité des SI

- Les menaces

Cybercriminalité

Services d'Etats
Organisations privées
Organisations terroristes



Script kiddies

Hacktivistes

Les enjeux de la sécurité des SI

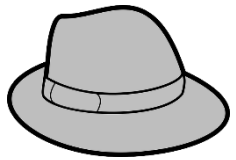
- Les hackers

  - Personnes à compétences techniques élevées (expert)
  - Classifiées en trois catégories White hat, Grey hat et Black hat
  - Recherche des vulnérabilités non publiées (Zero-Day)
  - Le hacker construis et/ou mène des attaques ciblées
  - Disposent de connaissances avancées
    - Programmation
    - Architecture matérielle
    - Administration système
    - Administration réseaux
    - Sécurité informatique

Les enjeux de la sécurité des SI

HACKERS

- Hacker éthique
- Agit dans la légalité et la moralité
- Effectue des test de vérification (PENTEST) de la sécurité
- Publication des vulnérabilités



- Hacker éthique ou non (voir idéologiste)
- Recherche des vulnérabilités
- Propose aux éditeurs de corriger avant publication des vulnérabilités

- Hacker malveillant (en groupe ou non)
- Mercenaire souvent associé à la cyber criminalité (ou état ?)
- Non Publication et monétisations des vulnérabilités

Les enjeux de la sécurité des SI

- Les scripts Kiddies

  - Personnes à compétences faibles utilisant des "tutos"

    - Tentative d'infiltration de système en utilisant des scripts
    - Attaque, vol de données, déni de service, défiguration
    - Jeux
    - Défis
    - Inconscient de l'impact
    - Peuvent être vecteurs d'attaque malgré eux
    - Différent des "Hackers"

      - Menace réelle difficilement contrôlable

Script kiddies

Les enjeux de la sécurité des SI

- Les hacktivistes

  - Accès sur des idéologies politiques, sociétales, religieuses, écologiques …
  - Un des plus connus : Edward Snowden
  - Mouvement des Anonymous
    - Personnes sans liens qui adhèrent ponctuellement à action
  - Les modes d'action :
    - Déni de service
    - Vol et divulgation d'informations sensibles
    - Défacement de site web (Modification de la page d'entête)

Les enjeux de la sécurité des SI

- Les services d'état ou organisation privée

  - Espionnage et contre-espionnage
  - Déstabilisation d'état ou de secteurs étatiques (Civil, militaire, justice..)
  - Attaque contre les OIV (Opérateurs d'importance vitale)

    - Attaques :
      - très évoluées et indétectables
      - Furtives
      - Reproduction, évolution et disparition programmées
      - Sabotage
      - Déstabilisation politique

  - Aucun outil conventionnel de sécurité ne permet de déceler ce type d'attaque

Les enjeux de la sécurité des SI

- Exemples d'attaque:

Nom	Type	Effet	Cible	Période
Shady Rat	Espionnage	Extraction de données + de 72 entités USA	Gouvernementsou association	2003 à 2006
Nuit de bronze	Sabotage	DDOS nombreux sites Web gouvernementaux et industriels	Estonie	27 avril 2007
Shamoon	Sabotage	Effacement de 30000 Disques (attaque par fichier image)	Compagnie nationale saoudienne hydrocarbure	15 août 2012 au 1er septembre
Stuxnet	Sabotage	Dysfonctionnements centrifugeuses uranium de Natanz	Iran	23 juin 2009 au mai 2010
TV5 Monde	Sabotage	Paralysie des moyens de diffusion	TV5 Monde	8 au 9 avril 2015
NotPetya	Sabotage	Destruction des SI utilisant un logiciel de comptable ME.DOC	Ukraine	27 juin 2017

Les enjeux de la sécurité des SI

- Gains financiers (accès à de l'information, puis monétisation et revente)
  - Utilisateurs, emails
  - Organisation interne de l'entreprise
  - Fichiers clients
  - Mots de passe, N° de comptes bancaire, cartes bancaires

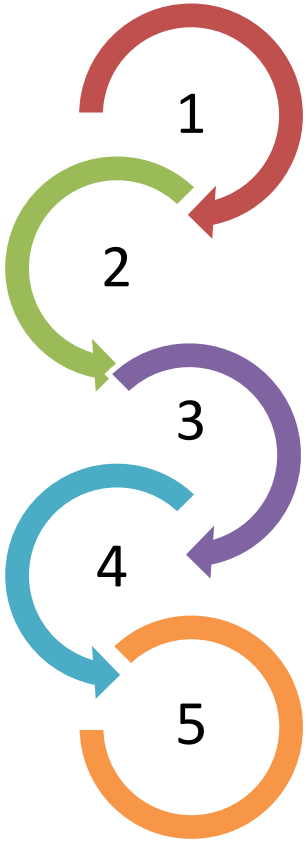
Cyber Criminel

- Utilisation des ressources
  - Bande passante et espace de stockage (hébergement de musique, films et autres contenus)
  - Zombies (botnets)
- Chantage
  - Déni de service ou modifications des données
- Espionnage
  - Industriel (technologie) ou concurrentiel (Tarifs)

La cybercriminalité

- L'industrialisation de la cybercriminalité

➡ Majorité des actes de délinquances sont commis par des groupes criminels organisés



Groupe développement : Programmes malveillants et virus

Groupe exploitation et commercialisation : Services d'attaque

Hébergeurs malveillant ou victime : Stockage des contenus illicites

Groupe de ventes : Données personnelles, bancaires et industrielles

Intermédiaires financiers : Collecte de l'argent

La cybercriminalité

- Quelques chiffres de l'économie de cybercriminalité

2 à 10 $	prix moyen de commercialisation des **numéros de cartes bancaires** en fonction du pays
5 $	Tarif de location pour 1 heure de **botnet** (Attaque WEB)
2399 €	Prix d'un **malware** "Citadel" permettant l'interception de numéros de carte bancaire

La cybercriminalité

- Quelques exemples d'attaques

Bug informatique à La Poste : "Tout est rentré dans l'ordre"

par **Caroline Piquet**
le 30 juillet 2013 à 15h50 , mis à jour le 30 juillet 2013 à 18h59.

A la suite d'une panne informatique, les opérations de prélèvements et de virements bancaires accusent un retard de 24 heures. Ce mardi, les clients ne pouvaient accéder à leurs soldes sur Internet et il leur était impossible de retirer de l'argent aux distributeurs automatiques.

Des machines à sous vidées à cause d'une faille informatique

Le Monde.fr | 15.04.2014 à 09h09 • Mis à jour le 15.04.2014 à 10h46

Abonnez-vous à partir de 1 € | Réagir | Classer | Partager

Hacker un pacemaker, c'est possible et c'est dangereux

10:12 - vendredi 19 octobre 2012 - Par Johann Mise - Source : France Info

Zoom

La cybercriminalité

- Attaque de Sony Pictures Entertainment en 2014

« *Si vous n'obéissez pas, nous publierons au monde les informations suivantes* ». Ce message était affiché sur plusieurs ordinateurs de Sony Pictures Entertainment le 24 nov 2014

- Attaque par le groupe Guardian of PEACE
- Attaque probable par la Corée du Nord
  - ➡ Publication de données internes sensible
    - ➡ Numéro de sécurité sociale
    - ➡ Numérisation des passports
    - ➡ Mots de passes internes
    - ➡ Scripts de cinéma confidentiels
    - ➡ Plans marketing
    - ➡ Données financières
    - ➡ Des films entiers inédit

Source : http://www.tomsguide.com/us/biggest-data-breaches,news-19083.html

La cybercriminalité

- Attaques ciblant l'enseignement

Tutoriels
Forum Général
Forum ForEva
Contacts

Espace étudiants

Ce Forum est un espace ouvert de communication entre étudiants, tuteurs, moniteurs et enseignants pour discuter des cours, des exercices, des travaux pratiques.

> **Poster un nouveau message** <

Liste des messages postés
pages 1 2 3 4 5 6 7 8 9 10

 # HACKED BY SWAN HACKED BY SWAN HACKED BY SWAN HACKED BY SWAN HACKED BY SWAN HACKED BY SWAN

Défacement de site

Click2Houston.com

Police: Student Installs Device On Teacher's Computer To Sell Tests

Warnings Sent To Other School Districts

POSTED: 5:23 pm CST February 1, 2005
UPDATED: 5:39 pm CST February 1, 2005

HOUSTON -- A high school student is facing criminal charges for allegedly hooking a device up to a teacher's computer to steal test information to sell to other students, Local 2 reported Tuesday.

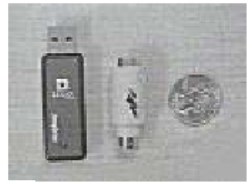
The student attended Clements High School, 4200 Elkins Dr., in the Fort Bend Independent School District.

Officials said the 16-year-old boy hooked up a keystroke decoder to a teacher's computer and downloaded exams in November.

"Sometime in mid-December, we got a tip that this student was selling test exams that had apparently come from a teacher's computer, so that's when the investigation began," said Mary Ann Simpson, with the Fort Bend School District.

The student confessed when he was confronted, officials said.

Video



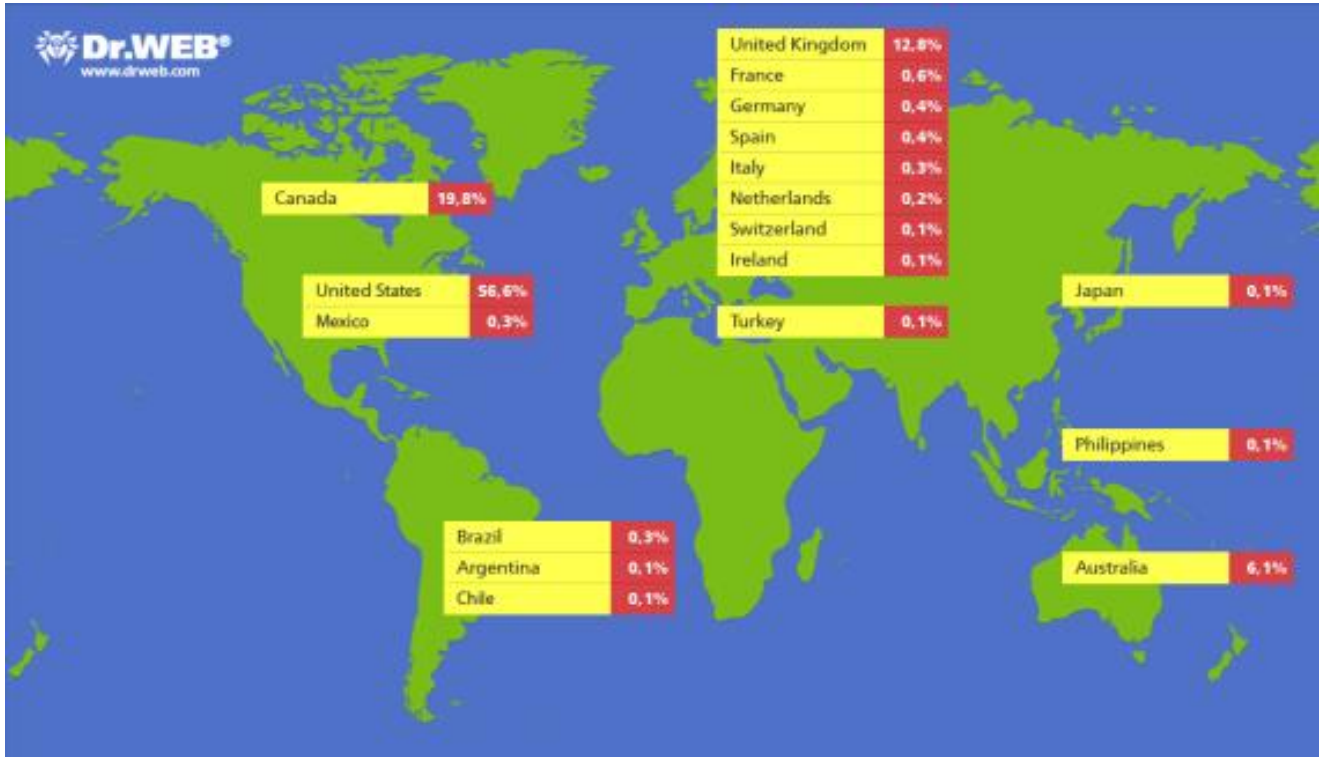
See How Keystroke Decoder Works

Vol de données d'enseignants

La cybercriminalité

- Attaque mondiale

  - BotNet FLASHBACK uniquement sur MAC OSX
    - 600 000 Ordinateurs infectés (via Fake Flash Player)
    - Vecteur d'infection : + 4 000 000 de pages web compromises



La cybercriminalité

- Attaque mondiale

  - Cryptolocker (Ransomware) Wannacry mai 2017
    - 300 000 Ordinateurs dans 150 pays en 4 jours
    - Utilisation d'outil de la NSA (EternalBlue)
    - Rançon de $300 à $600
    - Impact sur des grandes entreprises
      - Renault
      - FedEx
      - Deutsche Bahn

La cybercriminalité

- Attaque mondiale

  - Cryptomineur WinStartNssminer mai 2018
    - 500 000 Ordinateurs en 3 jours
    - Utilisation des ressources pour minage BitCoins
    - Plantage de la machine en cas de tentative de blocage
    - Similaire à un Mod compromis du jeux GTA 5

Source: ©360 Total Security

La cybercriminalité

- Le futur

  - Cyberattaques sur la voiture connectée (2020..)
    - Prise de contrôle du système de freinage
    - Anticipation avec module hardware HSM (Hardware Security Module)

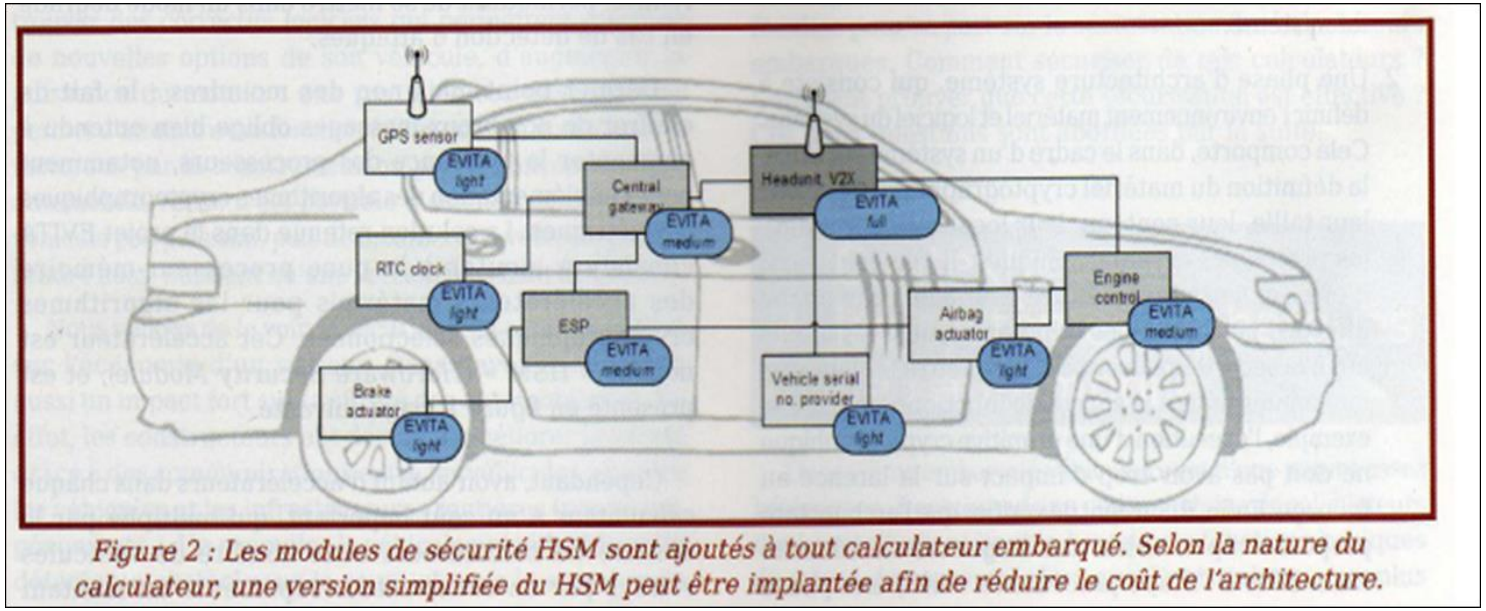
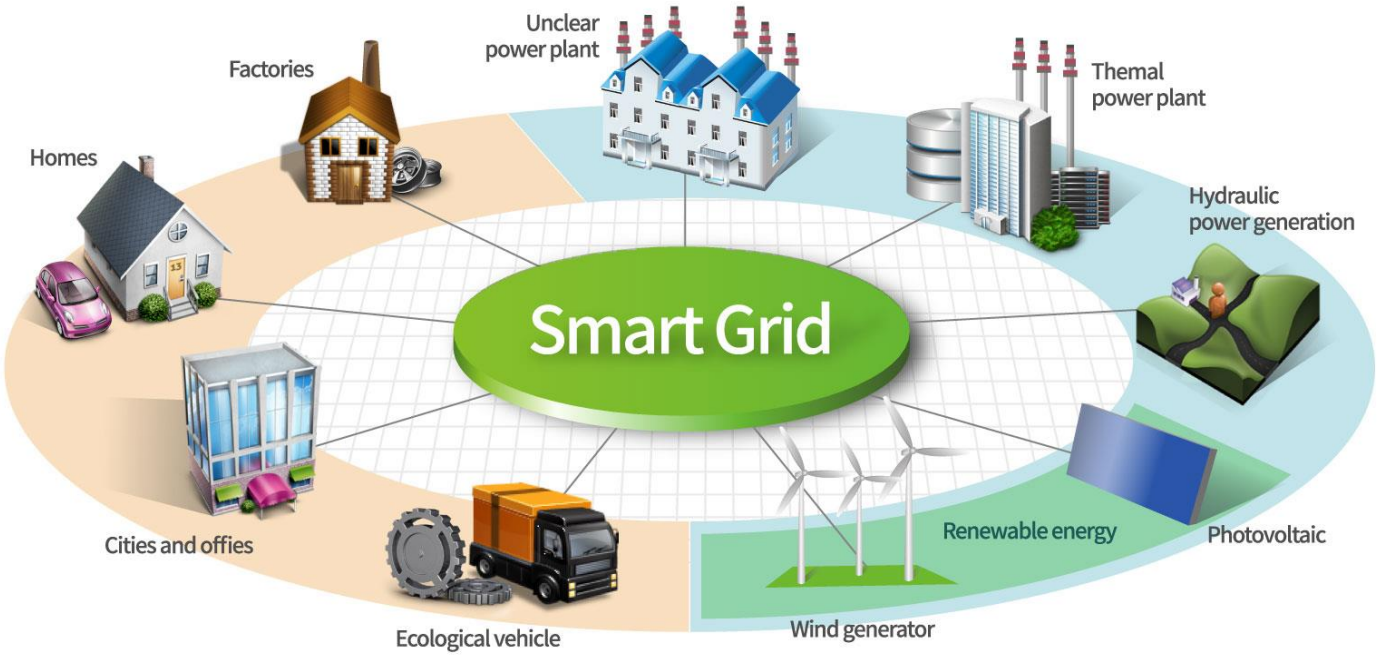


Figure 2 : Les modules de sécurité HSM sont ajoutés à tout calculateur embarqué. Selon la nature du calculateur, une version simplifiée du HSM peut être implantée afin de réduire le coût de l'architecture.

Les attaques de grandes ampleurs

- Le futur

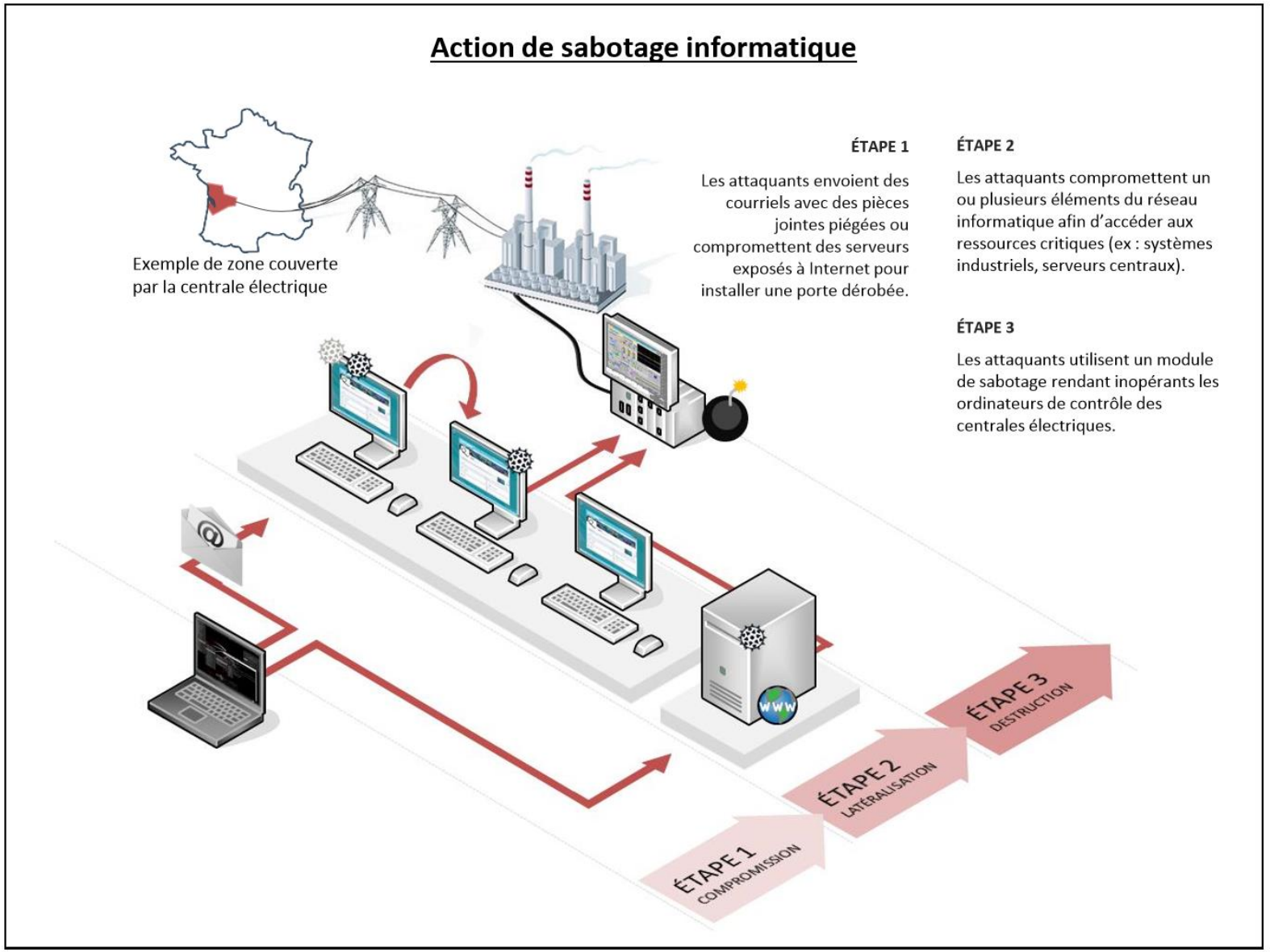
  - Cyberattaques sur les smart Grid (2030..)
    - Blackout complet sur une grille d'alimentation électrique



Source : https://les-smartgrids.fr

Les attaques de grandes ampleurs

- Scénario



Source : Revue stratégique Cyberdéfense

Panorama des menaces

- Les menaces courantes

Hameçonnage et ingénierie sociale

Fraude interne

Violation d'accès

Virus informatiques

Déni de service distribué

Panorama des menaces

- Hameçonnage (Phishing)
  - Attaque de masse par abus de la naïveté
    - Réception d'un mail avec logo de l'entreprise
    - Demande de mise à jour du mot de passe ou des données personnelles
    - Lien vers un faux site identique à l'original contrôlé par l'attaquant
    - Vol des identifiants/mot de passes saisies sur le site

Panorama des menaces

- Ingénierie sociale
  - Attaque ciblée des employés d'une entreprise
    - Vol d'informations sensibles ou vol d'argent (ex: Fraude au président)
    - Mise en place de logiciel malveillant dans le système d'information
    - Vecteur d'infection

Téléphone

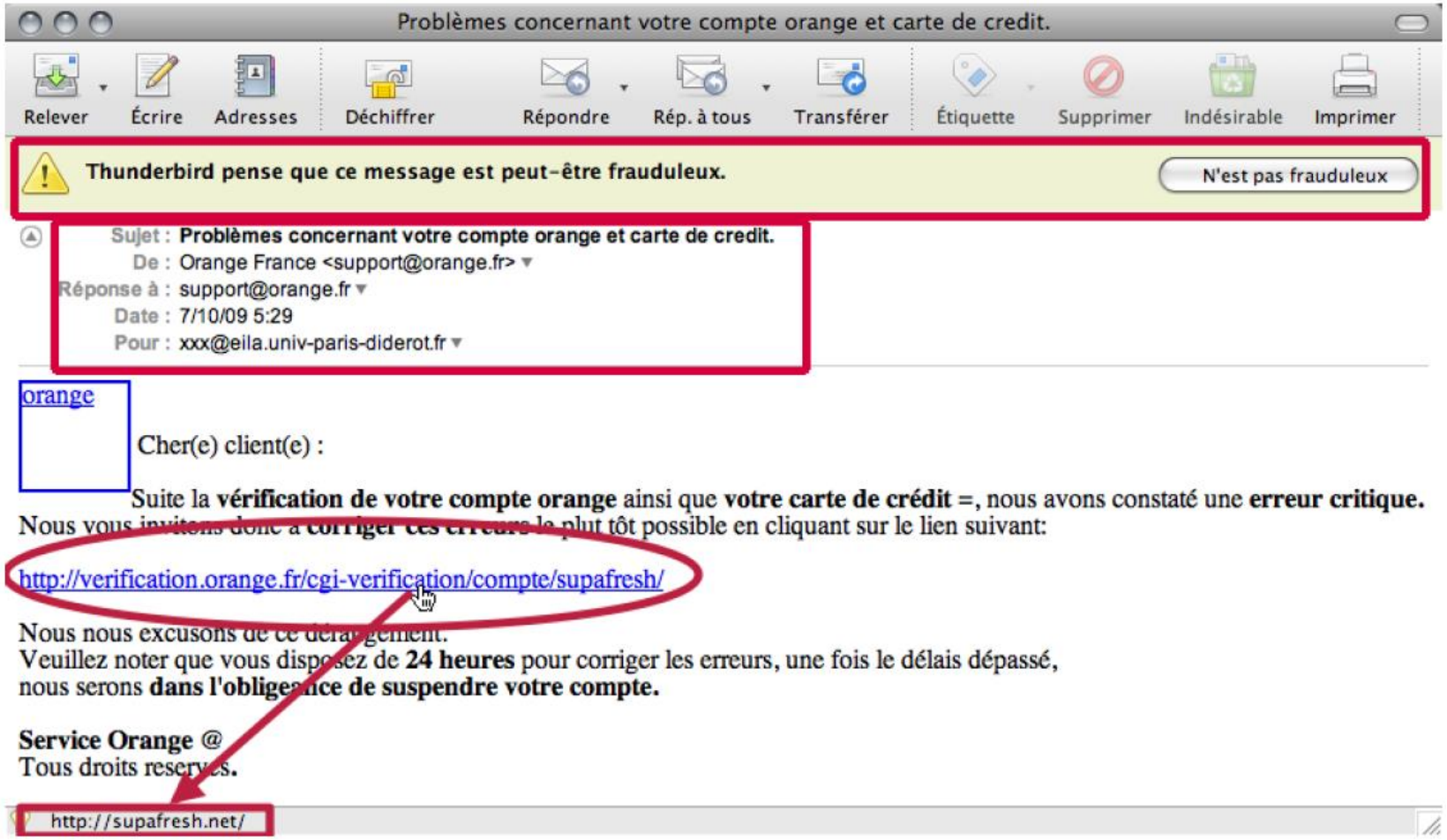
Réseaux sociaux

e-mail

    - Scénarios illimités utilisant une phase de collecte d'information et utilisant la méconnaissance et/ou la naïveté des employés

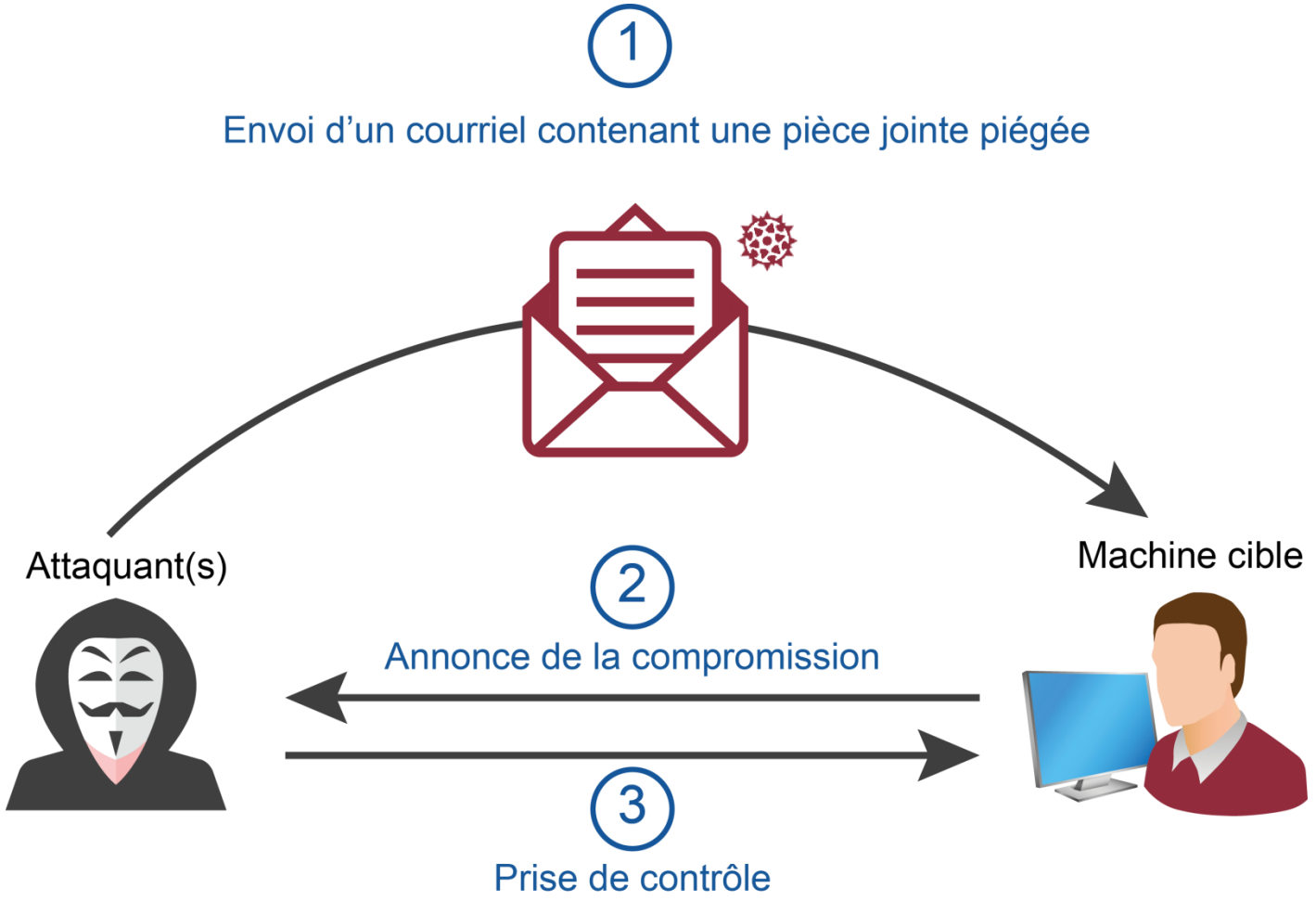
Panorama des menaces

- Exemple d'hameçonnage et d'ingénierie sociale combinée
  - ➡ Attaque ciblée du groupe ORANGE



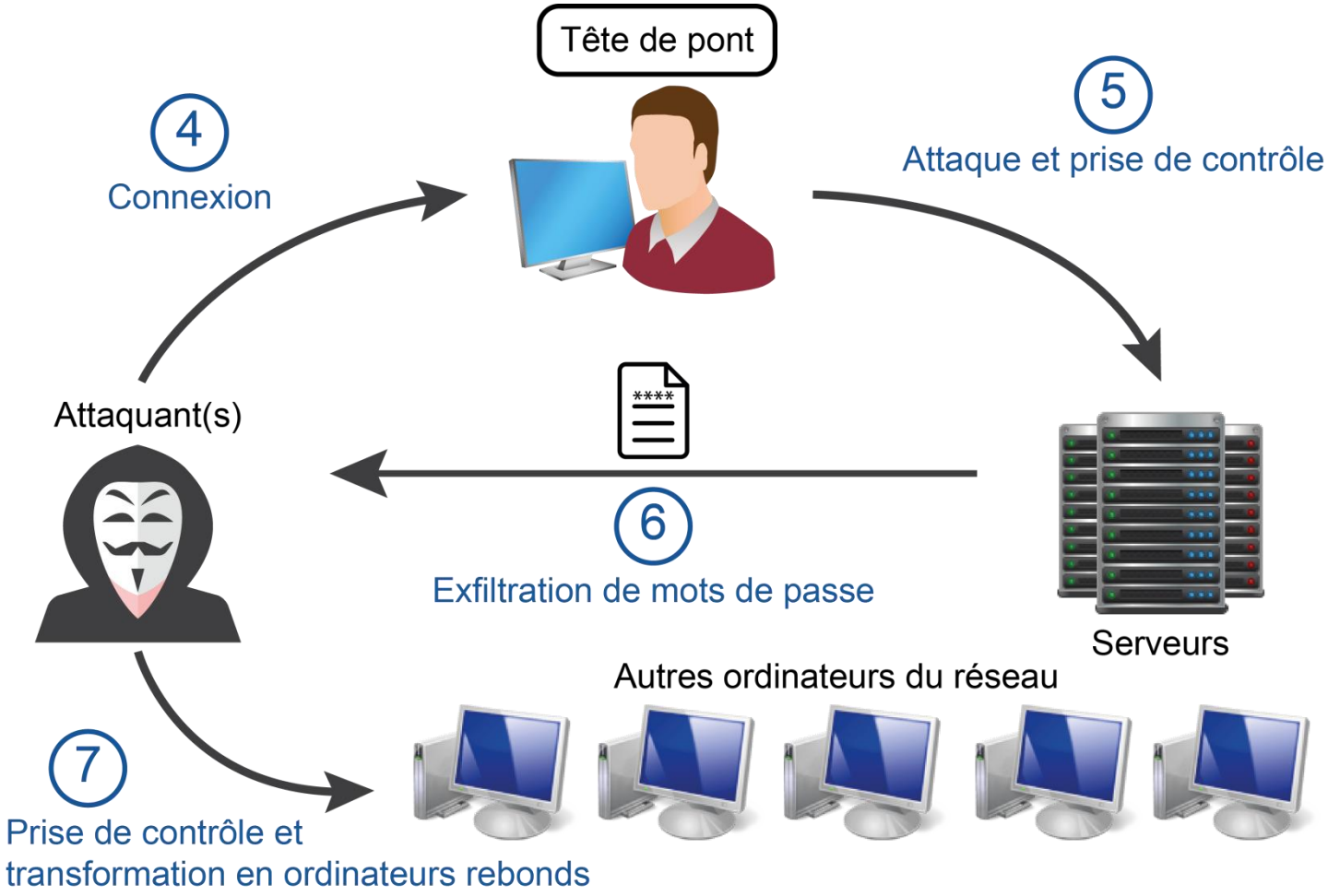
Panorama des menaces

- Déroulement d'une attaque avancée
  - ➡ Prérequis : étude d'ingénierie sociale sur l'utilisateur de la machine cible (Réseaux sociaux, partage ..)



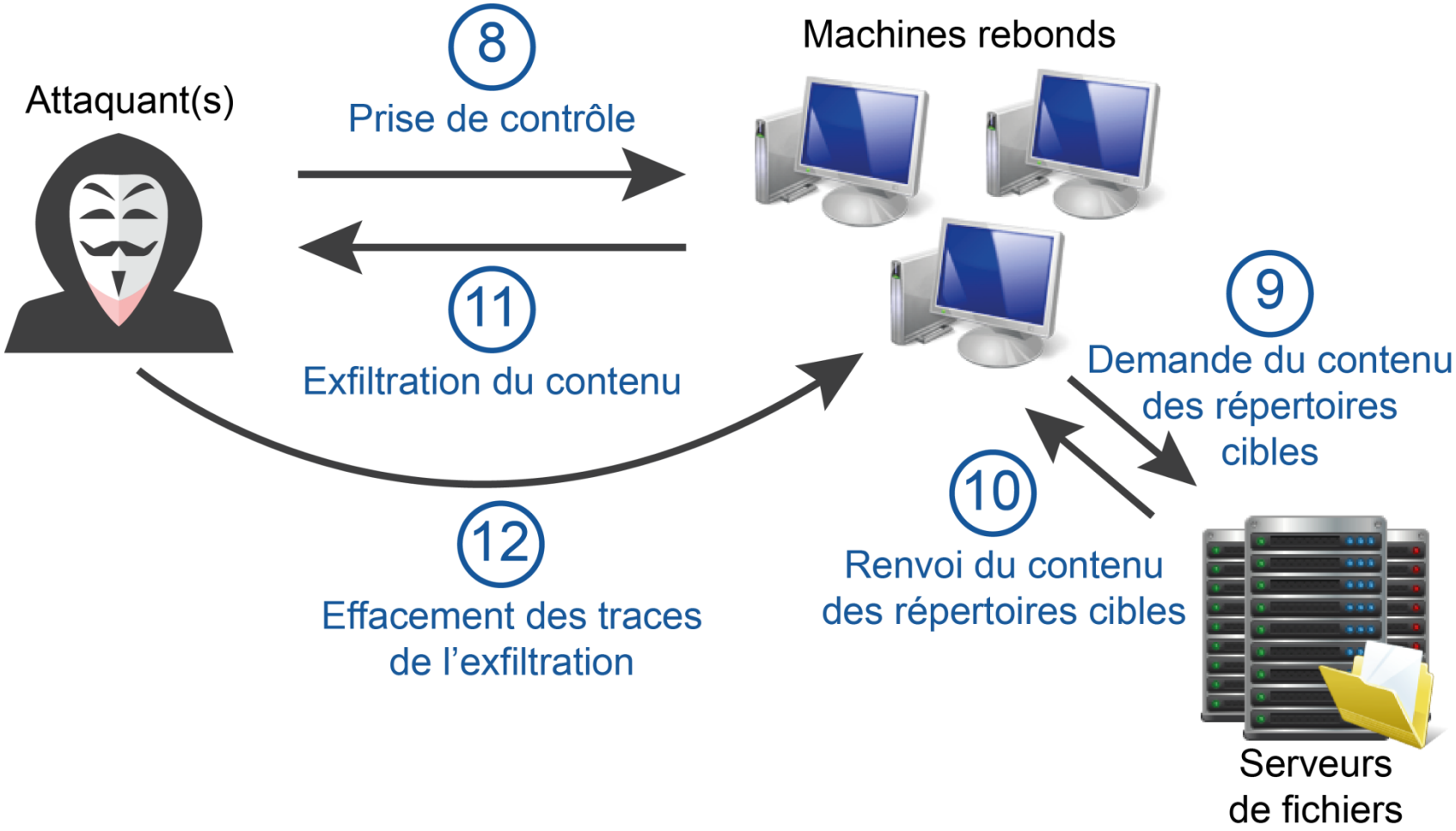
Panorama des menaces

- Déroulement d'une attaque avancée



Panorama des menaces

- Déroulement d'une attaque avancée



Panorama des menaces

- Fraude interne
  - ➡ Peu de communication de la part des entreprises (Sujet 'Tabou')

Catégories de fraudeurs

- Fraudeur occasionnel
- Fraudeur récurrent (petites sommes de manière régulière)
- Personne qui se fait embaucher pour effectuer une fraude
- Fraude en groupe

Vulnérabilités

- Faiblesse des procédures de contrôle interne et de surveillance des opérations
- Gestion permissive des habilitations informatiques
- Absence de séparation des tâches et de rotation

Typologies des fraudes

- Le détournement des avoirs de la clientèle
- Le détournement des avoirs de l'entreprise
- La création de fausses opérations
- La personne qui fausse ses objectifs pour augmenter sa rémunération

Violation d'accès

Panorama des menaces

- Accès non autorisé par mot de passe
  - ➡ Souvent lié à des mots passes faibles
  - ➡ L'utilisateur ne peut pas mémoriser beaucoup de mots de passe
  - ➡ Les attaquants utilisent des outils pour tenter de "casser" des mots de passes (John the ripper)
  - ➡ On peut rajouter des nouveaux moyens d'identification (Biométrie, SMS, One time password …)

Violation d'accès

Panorama des menaces

- Accès non autorisé par intrusion

  - Souvent des attaques ciblées exploitant des vulnérabilités techniques

    - Depuis le réseau internet via de ressources exposées (Web, partage etc..)
    - Depuis le réseau interne via un Active Directory ou des applications sensibles

80% des domaines Active Directory sont compromis en 2 heures

75% des domaines Active Directory contiennent au moins 1 compte privilégié avec un mot de passe trivial

50% des entreprises sont affectées par un défaut de cloisonnement de ses réseaux

80% des tests d'intrusion ne sont pas détectés par les équipes IT

Sources : tests d'intrusion Orange Consulting 2012-2013

Panorama des menaces

- Définition

  - Programme informatique malveillant destiné à se propager, se reproduire et exécuter une ou plusieurs actions (MALWARE)
  - Utilise généralement des failles de sécurité pour propager sa charge (PAYLOAD)
  - Très souvent pour des attaques massives

  - Classement en fonction de son mode propagation, de son déclenchement et sa charge :
    - Vers
    - Cheval de Troie
    - Macrovirus
    - Spyware
    - RootKits
    - Ransomware
    - …

Panorama des menaces

- Historique des malwares

  - Premier virus (Elk Cloner) en 1982 sur la plateforme APPLE II
    - Affichage d'un message et arrêt de la machine
  - Vers informatique (Morris Worm) en 1988 sur plateforme UNIX qui se propage par internet
    - Perturbation de service
  - Premier virus destructeur (Michelangelo) en 1991 sur plateforme DOS
    - Effacement de données
  - …
  - Concerne de nos jours tous les systèmes d'exploitation les plus courants

  - > 300 000 virus et variantes chaque jours

Panorama des menaces

- **Vers informatiques**
  - Faculté d'autoreproduction
  - Propagation par les réseaux en utilisant des protocoles distants (RPC, Rlogin,SMTP…)
  - Embarque une charge malveillante (PAYLOAD)
  - Vecteur d'infection
    - E-mail avec pièce jointe ou lien vers un site web infecté
  - Vecteur de propagation
    - Transfert de l'e-mail à tout le carnet d'adresse de la messagerie
- **Cheval de Troie**
  - Pas d'autoreproduction
  - Souvent utiliser pour créer des backdoor
  - Vecteur d'infection
    - Un faux programme légitime comme hôte
  - Vecteur de propagation
    - Site web "catalogue" de logiciel non officiel

Panorama des menaces

- **Macrovirus**
  - Exécution uniquement d'un environnements logiciel spécifique (OFFICE..)
  - Vecteur d'infection
    - Fonctionnalité "Macro" des logiciels
  - Vecteur de propagation
    - E-mail avec document infecté en pièces jointes

- **Logiciel espion (Spyware)**
  - Collecte d'informations à l'insu de l'utilisateur
  - Vecteur d'infection
    - Logiciel "Gratuit", logiciel "Piraté", logiciel de "sécurité" de type CCleaner
  - Vecteur de propagation
    - Magasin de logiciel en ligne (Apple store, Google Play)

Panorama des menaces

- **RootKits**
  - Boite à outils (pré-OS) qui permet à un pirate de prendre le contrôle administrateur d'une machine
    - Enregistreur de frappe (Keylogger), Capture de mot de passes et carte bancaire
    - Désactivation des logiciels de sécurité
  - Vecteur d'infection
    - Vulnérabilité système, logiciel "Piraté", clé USB, site web

- **Cryptologiciel (Ransomware)**
  - Chiffre les données de l'utilisateur et demande une rançon pour déchiffrer
  - Paiement par virement, sms surtaxé, BitCoins
  - Vecteur d'infection
    - Cheval de Troie, site web avec contenu illicite, logiciel "Piraté", e-mail

Déni de service distribué

Panorama des menaces

- Distributed Deni Of Service
  - Attaque ciblée
  - Objectif : saturer un service web par un nombre de requêtes très important
  - Utilisation de réseaux de machines infectés

- 34,5 heures durée moyenne d'une attaque
- 48,25 Gbps bande passante moyenne d'une attaque
- 75 % des attaques au niveau infrastructure, 25% des attaques au niveau application

Aspect juridique de la sécurité des SI

- LOI "Godfrain" du 05 janvier 1988

  - Article 323-1 et s du code Pénal

    - Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de **deux ans d'emprisonnement** et de **60 000 euros d'amende.**

    - Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de **trois ans d'emprisonnement** et de **100 000 euros d'amende**

Aspect juridique de la sécurité des SI

- LOI "Godfrain" du 05 janvier 1988

  - Précise les éléments suivants :

    - **Accès passif** : Analyse statique, capture de trafic réseau, enquête..

    - **Accès actif** : utilisation d'une faille, blocage du SI, vol de donnée, défiguration de site web…

    - **Maintien frauduleux** : acte volontaire indépendant de l'erreur d'inadvertance

FIN