Edmonium

Introduction à la cybersécurité par quelques exemples

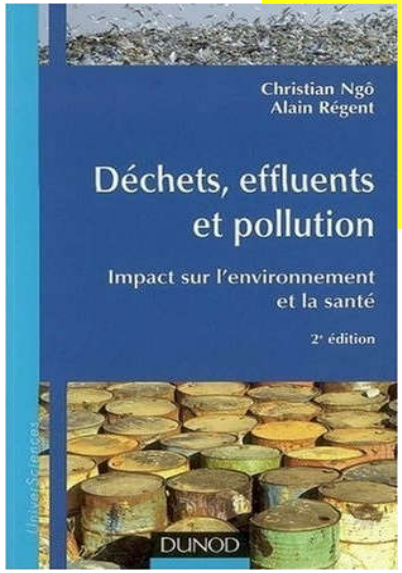
Christian Ngô

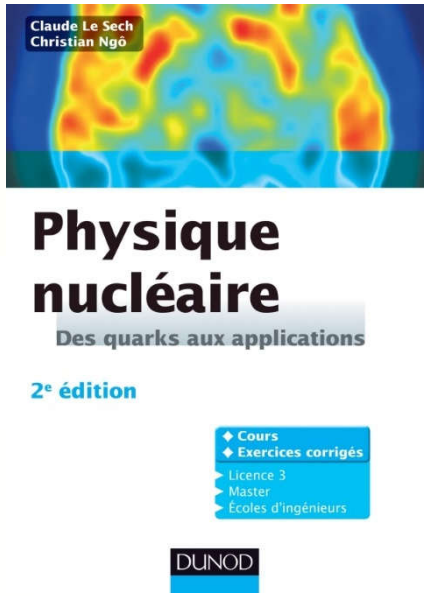
Edmonium

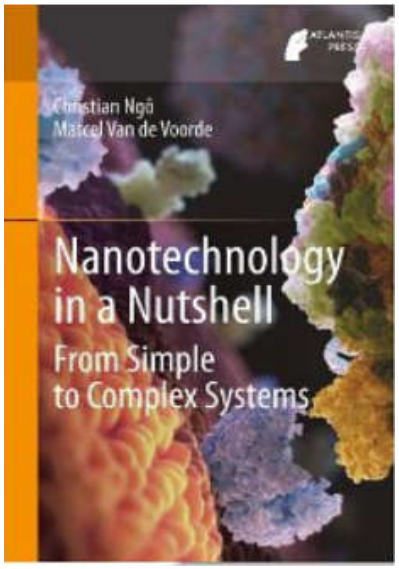
edmonium@gmail.com

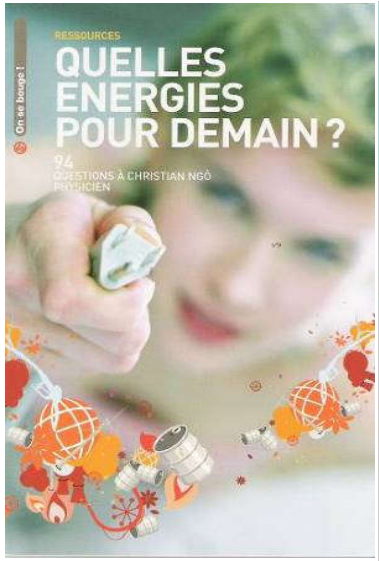
www.edmonium.fr

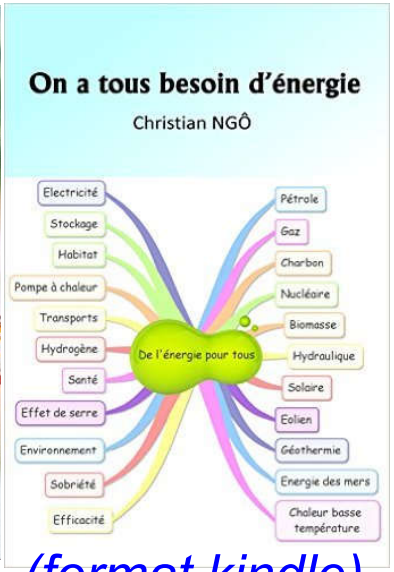
http://edmonium.wordpress.com/

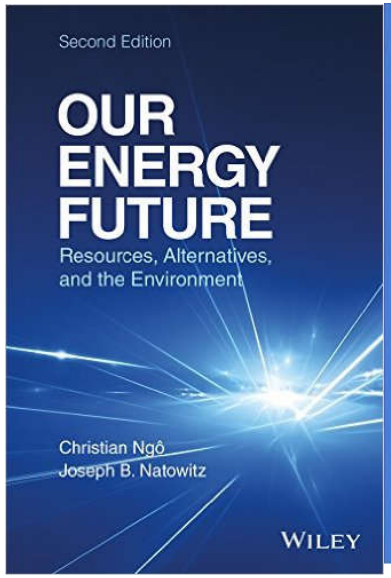


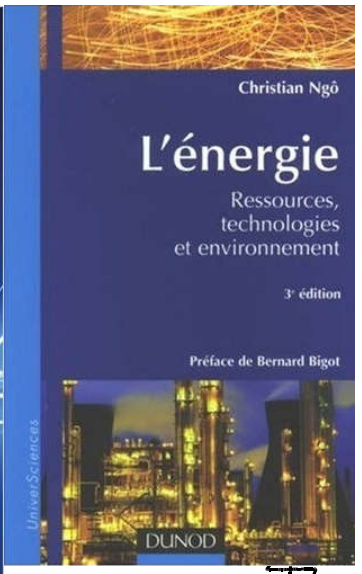












(format kindle)

Edmonium

Vulnérabilités

L'actif d'une entreprise comprend : les équipements matériels et logiciels, les brevets, les connaissances des processus, les fichiers clients, etc.
Ils ont tous une valeur pour l'entreprise

Vulnérabilités (vulnerability) ⇒ faille dans les actifs, les contrôles, les procédures
Menaces (threat) ⇒ exploiter une vulnérabilité
Contre-mesures ⇒ avant, pendant et après

吳

Edmonium

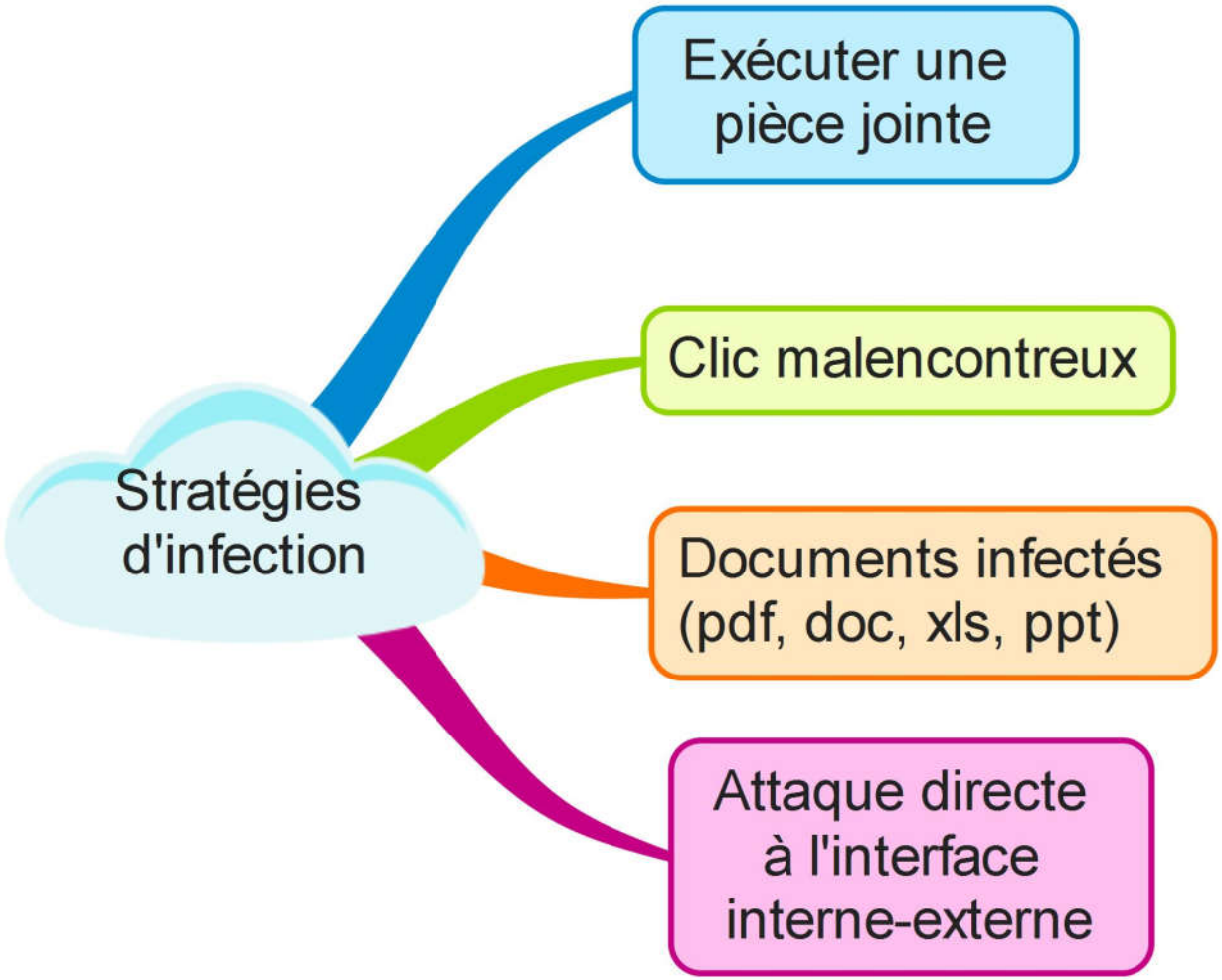
Malwares

Un malware est un logiciel malveillant permettant de compromettre un système informatique à l'insu de son propriétaire

Années 1970 : premiers malwares
Creeper ⇒ utilisait un modem et affichait : « I'm Creeper; catch me if you can ».
Depuis les malwares sont devenus beaucoup plus dangereux (exemple Stuxnet (centrifugeuses d'Iran) ou Flame en 2012)
Flame est resté en activité pendant des années sur des ordinateurs sans qu'on le sache. Il pouvait :
Collecter des informations, changer à distance les réglages, activer le micro, enregistrer des conversations, se connecter à des messageries instantanées, etc.
Il s'agit sans doute d'une cyberarme développée par un état (USA, Israël?).

Edmonium

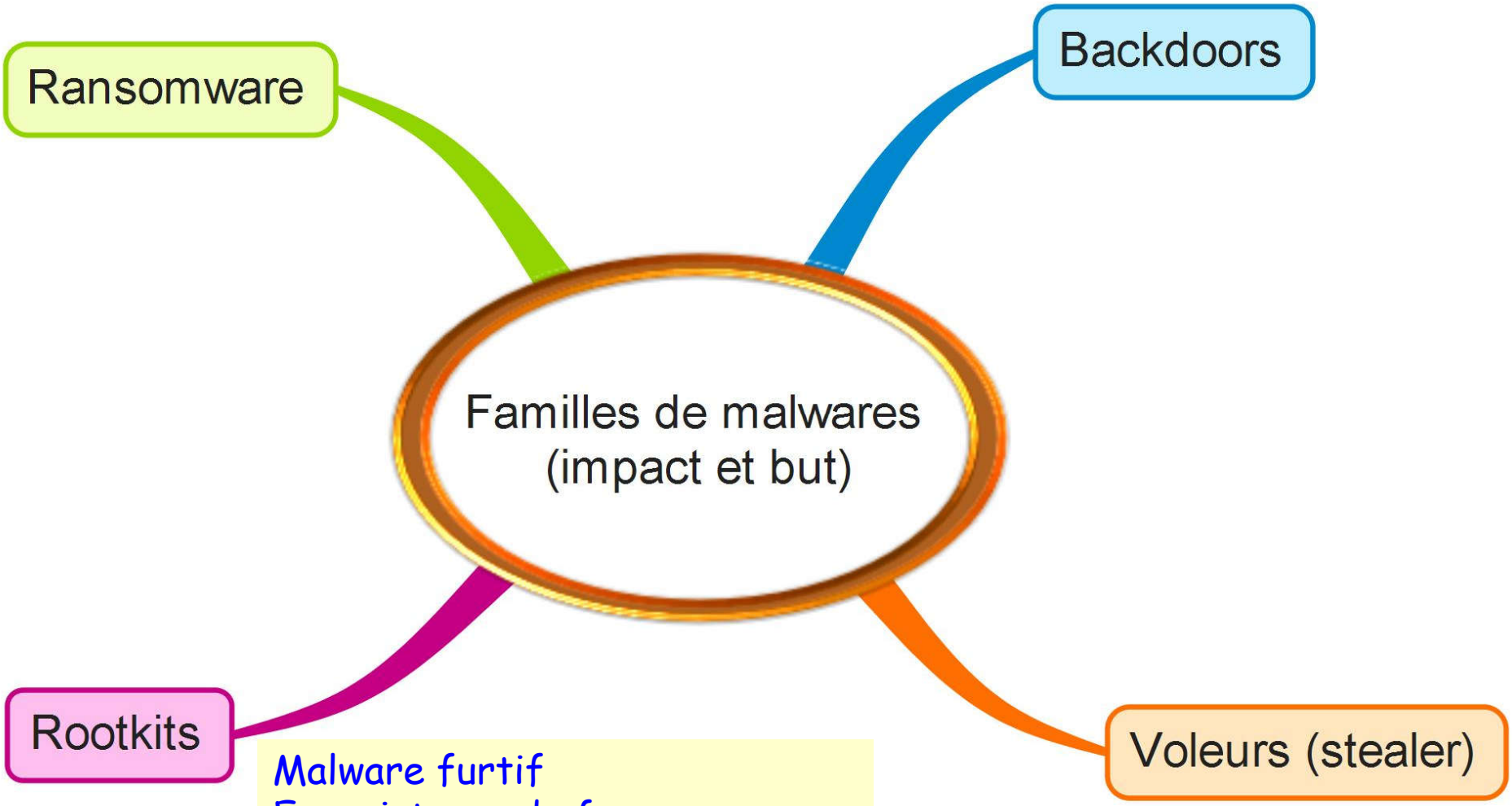
Exemple : Ver informatique Duqu Découvert le 1/9/2011. Il est très proche de Stuxnet et sophistiqué. Vole des informations sensibles



Attaque Windows grâce à une vulnérabilité zero-day.
Objectif : recueillir des infos sur les systèmes industriels pour préparer une attaque
Origine : Services secrets israélien ?

呆

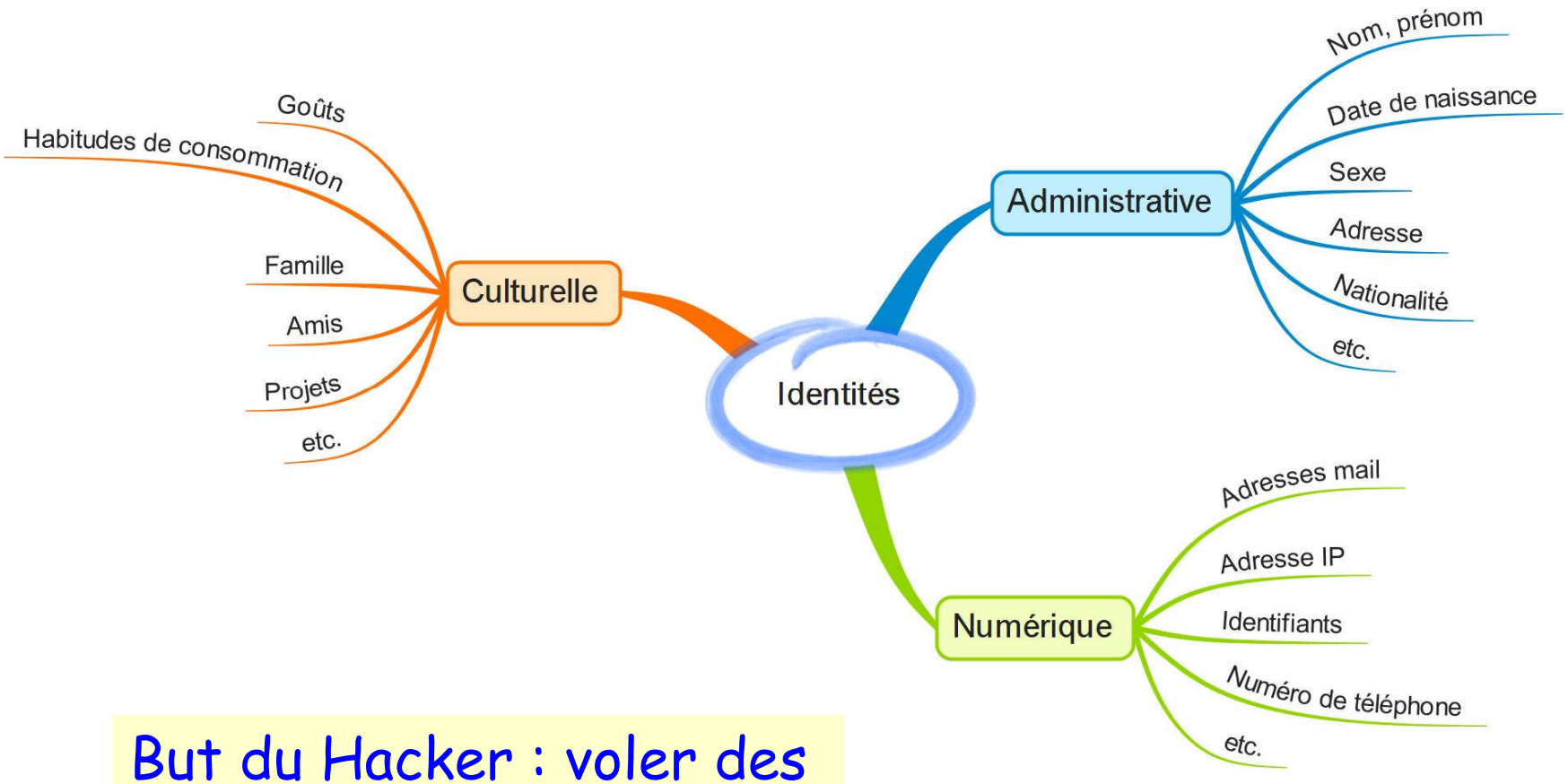
Edmonium



Malware furtif
Enregistreur de frappe
Vol d'informations bancaires
Vol de mots de passe
Transformation en botnet pour attaque DDOS

吳

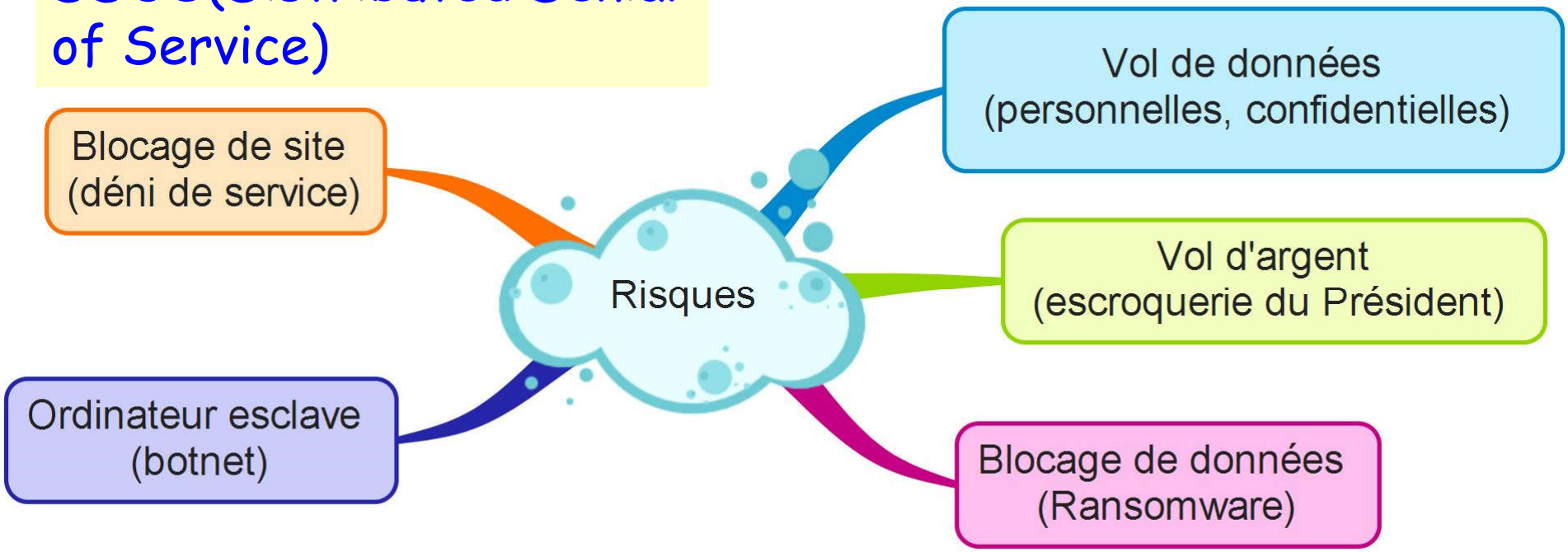
Les identités



But du Hacker : voler des informations pour les monétiser

Edmonium

Attaques DOS (Denial of service) et DDOS(Distributed Denial of Service)



Les attaques sont automatisées

Tout ordinateur connecté à internet ou à un réseau externe est susceptible d'être attaqué.

- Le pirate scrute réseau de manière aléatoire en envoyant des paquets de données.
- S'il voit un ordinateur connecté il cherche les failles

→ Il faut se protéger

- Antivirus
- Firewall (pare-feu)
- Proxy
- Zone démilitarisée (DMZ)

Edmonium

Les dégâts sur quelques exemples

- Le but des personnes qui utilisent les virus aujourd'hui est de gagner de l'argent (ex. ransomwares) ou, dans le cas d'une attaque faite par un État de perturber, détruire, contrôler des systèmes informatiques et des installations industrielles, financières, etc.
- 2007 : cyberattaque DDOS de l'Estonie (sites officiels, banques, médias…) : pays complètement déstabilisé
- 2008 Attaque DDOS de la Géorgie qui neutralisent toutes les infrastructures du pays.
- May 2011 Lockeed Martin paralysé pendant quelques heures et codes de sécurité volés
- 2017 (Wannacry, NotPetya, Adylkuzz). Sociétés touchées : Renault, Auchan, FedeX, Saint-Gobain, etc.
- Environ 180 000 cyberattaques/jour dans le monde

Edmonium

Les malwares (maliciels)

Programme ou morceau de programme qui perturbe, altère ou détruit des parties d'un système informatique. (CPA = code autopropageable)

- Les virus TSR (Terminate et Stay Resident) se chargent en mémoire centrale et infecte les fichiers qui sont exécutés
- Les virus non résidents infectent les programmes exécutables qui sont sur le disque dur dès leur exécution
- Les Vers se propagent dans le réseau
- Les troyens ou chevaux de Troie (trojans) permettent de créer une faille dans le SI pour que l'assaillant puisse s'introduire dans le système et le contrôler à distance. Souvent troyens ne se reproduisent pas
- Les bombes logiques sont des virus qui se déclenchent lors d'un évènement particulier (date, activation à distance, etc.)

Edmonium

Les types de virus

- Virus mutants (réécrits par d'autres utilisateurs ce qui modifie leur comportement et leur signature)
- Virus polymorphes (changent de signature en temps réel). Ont une fonction de chiffrement déchiffrement de leur signature
- Rétrovirus (bounty hunter ou virus flibustier) peuvent changer les signatures des antivirus pour les neutraliser
- Virus d'amorçage (virus de boot). Infecte le secteur de démarrage du disque dur (MBR, Master Boot Record).
- Virus de macros (dans les documents utilisant du Visual Basic (VBScript) dans Word, Excel, etc.
- Sans doute une centaine de milliers de virus mais quelques milliers en circulation.

Edmonium

Antivirus

Un antivirus détecte et éradique les virus. Il ne détecte en principe que ceux qui sont connus (pas les zero day)

Malware
Fichier ou bout de code caché dans un fichier
Signature virale
On les repère par leur comportement. Chaque malware a une signature propre. On recherche cette signature (scanning) en utilisant une base de données. Mais ne détecte pas les zero day et les virus camouflés ou qui changent de structure (virus polymorphes)
Contrôle d'intégrité
Vérifie qu'il n'y a pas de fichier exécutable important modifié à l'insu du propriétaire

Edmonium

Les ransomwares ou rançongiciels

- Crypter les fichiers d'un ordinateur, en empêcher l'accès ou verrouiller le système d'exploitation
- Demande de rançon pour décrypter ou déverrouiller
- Ne pas payer car on n'est pas sûr qu'on aura la clef de déverrouillage en retour
- Se cache dans les mails, les pièces jointes, les macros de Microsoft office…
- Wannacry (mai 2017) a touché 300 000 ordinateurs et 150 pays. St Gobain : perte de 250 M€ (1% du CA). A utilisé un Web Exploit développé par la NSA (EternalBlue) et volé par les Shadow Brokers. Nombreuses sociétés touchées. Grosses pertes financières
- NotPetya (23 juin 2017). Destructeur de données mais aussi ransomware. L'entreprise de transport danoise Maersk a perdu 300 millions de $

Spywares (espiogiciels, mouchards)

Programme permettant de recueillir des informations sur l'utilisateur comme :

Sites web visités, mots-clés saisis dans les moteurs de recherche, analyse des achats effectués (parfois numéro de CB), informations personnelles (numéro SS, identité, etc.)

- Servent souvent à faire du profilage mais ils ralentissent l'ordinateur , peuvent planter des applications, ouvrir des fenêtres publicitaires
- Ils occupent de l'espace dans les boîtes aux lettres
- Il est difficile de consulter ses mails et on peut laisser passer des bons
- Ils font perdre du temps pour les trier et les supprimer

Edmonium

Spywares ⇒ Contremesures

- Les hébergeurs de mails mettent des filtres antispam
- On peut utiliser un filtre antispam mais cela alourdit la correspondance mail
- Le nombre de spam diminue (moins intéressant pour les spammeurs que d'autres techniques cybercriminelles) 60% de mails indésirables en 2015 contre 90% en 2010
- Démantèlement de botnets. Ex par Microsoff: botnet Waledac démantelé en 2010 (1,5 milliard de spams/jour). 2011 -> Rustock comprenait 1 million de botnets et avait généré 47% des spams mondiaux pendant 4 ans.
- En 2015 environ 8 spams/seconde au niveau mondial (50 spams/seconde début 2008)
- https://www.spamcop.net/spamgraph.shtml?spamstats

Le phishing (hameçonnage ou filoutage)

Obtenir des renseignements personnels en vue d'une usurpation d'identité

Chronopost.fr <info.chronopost@rumbodentro.com>

À moi

Chronopost vous informe que l'envoi de votre colis est en cours d'achévement.

- Nous avons l'honneur de vous informer par le présent que nous avons reçu un colis volumineux qui a été envoyé par votre expéditeur ce matin au bureau de poste et prêt à être livré à votre adresse de résidence ou en point relais.

- Nous revenons vers vous afin de vous informer qu'il est préferable de confirmer l'envoi de votre colis avant qu'il soit retourné a votre expéditeur.

- Veuillez confirmer l'envoi à domicile ou en point relais en suivant la procédure ci-dessous :

1

Appelez le service de confirmation Trois fois de suite:

N°:08 99 700 640

2

Vous allez recevoir le code de confirmation durant le troisiéme appel téléphonique.

3

Envoyez le code de confirmation a l'adresse mail suivante:

chronopost_service@workmail.com

Edmonium

Ingénierie sociale

Exemple d'attaque classique

Hacker ⇒ Alice
Objectif ⇒ collecter des informations confidentielles pour un groupe étranger

Étape 1 ⇒ Cible : Pierre (manager dans l'entreprise)

- Collecte d'informations sur lui et son entreprise (réseaux sociaux, forums, traces internet, etc.)
- Alice lui téléphone en se faisant passer pour une journaliste et en flattant son entreprise pour faire un article sur lui et son entreprise
- Avec toutes les informations recueillies, Alice va se faire passer pour Laura, collaboratrice dans une filiale de l'entreprise à l'étranger

吳

Ingénierie sociale

Exemple d'attaque classique (http://www.conscio-technologies.com)
https://www.youtube.com/watch?v=IbetgF2f_58

Edmonium

Ingénierie sociale

Précautions à prendre

吳

Vidéos sur les ransomwares

https://www.youtube.com/watch?v=e-6-o1NJU1g

https://www.youtube.com/watch?v=DJCZgeISpW4