

## La France et la cybercriminalité

*Publirelais a décidé de vous parler de la cybercriminalité dans notre pays car celle-ci inquiète et vous concerne. Veuillez trouver ci-dessous les informations que nous avons jugées intéressantes pour vous afin que vous puissiez vous protéger ainsi que votre travail.*

### Qu'est ce que c'est ?

La cybercriminalité est une action frauduleuse faite par un cybercriminel sur un ordinateur. Internet et l'ordinateur sont les outils de la cybercriminalité. Les smartphones seraient une nouvelle cible des cybercriminels.

### Forme de cybercriminalité :

- HACKING
- DENIAL OF SERVICE ATTACK
- VIRUS DISSEMINATION
- SOFTWARE PIRACY
- PORNOGRAPHY
- IRC Crime
- CREDIT CARD FRAUD
- NET EXTORTION
- PHISHING
- SPOOFING
- CYBER STALKING
- CYBER
- DEFAMATION
- THREATENING
- ALAMI ATTACK

### Risque :

Les entreprises peuvent se faire voler, détruire ou modifier les informations propres à son fonctionnement et ses données entreprises multinationale ou les institutions sont souvent soumises à ce type d'attaques car elles détiennent des informations qui peuvent avoir un fort intérêt financier.

■ En tant que consommateur le risque est plus centré sur les virus, la pornographie ou l'usurpation d'identité.

## Processus d'une intrusion sur ordinateur:

Généralement en deux temps.

- ▶ D'abord, la contamination : elle serait généralement faite via un courrier électronique muni d'une pièce jointe adressé à une personne en particulier peut-être même avec des détails sur sa vie privée rendant le message plus vraisemblable.
- ▶ Ensuite, l'intrusion proprement dite : la personne clique sur la pièce jointe car elle n'a pas de raison de se méfier de l'expéditeur. Dès lors, le mal est fait : le code malveillant va contaminer la machine ainsi que d'autres machines connectées et commencer à fouiller dans les disques durs sans rien dire ou inciter à transmettre des informations confidentielles comme le numéro de la carte bleue et son code secret.

Autres exemples de cybercriminalité : Le blanchiment d'argent et les attaques d'ordinateurs par exemple Google attaqué par des cybernautes chinois et récemment le ministère des finances par on ne sait qui.

## 5 menaces recensées pour 2011 :

-les réseaux sociaux est un nouveau vecteur de fuite d'informations sensibles car les arnaque à la carte bleue, arnaque qui est faite en se servant des infos "lâchées" sur les réseaux sociaux.

-L'IPv6 (internet protocole version 6) un tremplin pour les pirates, c'est-à-dire que votre adresse IP ne sera plus sous la forme 192.168.192.157 mais sous la forme 192.168.192.157.012.409. cela personnalise les adresses ip au point d'être presque nominatives dans une entreprise donc plus ciblé.

-Les Anonymous (collectif de pirates militant ou "hacktivistes") sont une menace pour les RSSI (Responsable de la sécurité des systèmes d'information)

-Smartphones et le mythe des OS sécurisés (systèmes d'exploitation, exemple Apple, Android, windows...) car plus l'OS est utilisé plus il est vulnérable. Le fait qu'il soit vulgarisé le rend intéressant pour les hackers.

-Des industries dans le collimateur des pirates (des hackers chinois se sont attaqués aux entreprises pétrières).

## Organismes et institutions françaises :

Le pays européen le plus attaqué par les pirates avec 1 attaque sur 25 est la France.

L'espionnage dont vient d'être victime Bercy en est un exemple notable. Il y eu 150 postes contaminés pendant 3 mois. La cible était le ministère de l'Economie et des Finances et des données concernant le G20.

C'est pour cela que les organismes suivant existent afin de protéger la France et ses cybernautes.

- ANSSI, La nationale de la sécurité des systèmes d'information
- Le forum international de la cybercriminalité
- l'OCLCTIC, la division de la police judiciaire,
- La LOPPSI établit une série de délits spécifiques s'ils sont exercés sur le Net
- La CNIL, Comité National de l'Informatique et des Libertés.
- Enisa, European Network and Information Security Agency.

On parle également de la cybercriminalité lors des réunions G8 comme l'a annoncé N. Sarkozy « son intention de réunir les principaux acteurs mondiaux de l'Internet en marge du sommet du G8 de Deauville, en mai prochain. L'inscription du sujet de la protection de la vie privée à l'ordre du jour du G8, qui se tiendra sous la présidence française, permettrait de franchir une étape décisive dans la protection de la vie privée face au développement des technologies du numérique et éclairerait le rôle déterminant que la France joue en la matière. »

Il existe aussi des conférences comme celle ci-dessous :

Lieu : Mercredi 16 mars, à 19h15 à l'Ecole Militaire, Amphithéâtre Lacoste.

Thème : "LA CYBERDEFENSE, UN EFFORT DE LA NATION DANS TOUTES SES COMPOSANTES"

Par : Comité Cyberdéfense, ANAJ-IHEDN et M. Florent Chabaud, Ingénieur en Chef de l'Armement, actuellement FSSI

(Fonctionnaire de Sécurité des Systèmes d'Information) du Ministère de la Défense, a été sous-directeur à l'ANSSI (SGDSN).

**Conseils :**

A faire :

-pour protéger l'ordinateur ou les ordinateurs d'une entreprise : Antivirus et pare feu (firewall)

-individuellement, faire attention aux protections des réseaux sociaux, attention à ce qu'on laisse dans les mails,

A ne pas faire : attention à ne pas enregistrer de mot de passe, de votre banque par exemples, sur votre ordinateur car la plupart des vols de ces mots de passe se fait par l'entourage "proche".

**Sources**

JDN, 14/03/11

<http://www.lefigaro.fr/actualite-france/2010/03/30/01016-20100330ARTFIG00475-l-europe-declare-la-guerre-a-la-cybercriminalite-.php>

<http://www.latribune.fr/actualites/economie/france/20110305trib000605992/comment-les-policiers-francais-traquent-les-cybercriminels.html>

<http://fr.fashionmag.com/news-159742-Google-veut-rassurer-via-des-mesures-anti-contrefacons>