BSCI
Bertrand SCHMERBER
Conseil en Informatique

La sécurité numérique
Les dangers pour votre PC

Pour mieux se défendre, il faut connaître ses ennemis, il faut donc évaluer les besoins et les risques encourus et chercher d'où peuvent venir les menaces

1. Les utilisateurs

Il arrive que le virus le plus dangereux soit assis juste en face de l'écran !

Les principaux risques viennent bien sûr du Web, mais beaucoup d'incidents sont aussi causés par les utilisateurs. Soyez donc prudent, parce que le premier utilisateur dangereux de votre PC c'est peut-être vous.

Posez-vous la question « qui peut accéder à mon PC en dehors de moi ? »

La réponse est « Quasiment tous ceux qui peuvent entrer dans le local où se trouve le PC. » et si vous n'avez pas de mot de passe suffisamment complexe ils peuvent le faire même si vous avez éteint la machine en partant.

Il vous faut donc un bon mot de passe et dans certains cas, une protection physique de votre PC (ou du local) contre d'éventuels bricoleurs indélicats

Il se peut que le PC soit partagé avec d'autres personnes, dans ce cas il est recommander de faire en sorte que chacun a son compte et son mot de passe indépendant. Pour les enfants, il est toujours préférable de ne jamais les laisser seuls jouer avec un PC jusqu'à ce qu'ils soient assez grands pour déjouer les dangers d'internet.

Mais il s y a aussi des dangers qui ne dépendent pas de vous (ou des autres utilisateurs) et que vous pouvez combattre, mais pour cela, il fardait que vous les connaissiez un peu mieux. Voici donc pour vous motiver, un petit échantillon des dangers qui guettent votre PC.

2. Les Pirates

Voici quelques exemples de méthodes que peuvent utiliser les pirates pour vous nuire !

- Déni de service :(Ddos ou distributed denial of service), technique qui consiste à saturer à haut vitesse un serveur web d'interrogations très nombreuses pour bloquer complètement la communication
- Rebonds : attaquer des serveurs, avec des machines non protégées (peut-être votre PC) l'utilisation frauduleuse de ressources : Intrusion extérieure (ou intérieure) pour copier les contenus du disque dur

- Le Phishing consiste à faire croire à la victime qu'elle s'adresse à un tiers de confiance (banque, administration, etc.) pour obtenir des renseignements personnels (mot de passe, numéro de carte de crédit, date de naissance, etc.) dans le but de commettre une escroquerie.

Pour se protéger contre les pirates communs il vous faudra essayer d'appliquer les règles de sécurité décrites sur ce site. Mais les vrais professionnels, tout comme les vrais casseurs de coffre-fort, trouverons toujours un moyen d'accéder au contenu de votre PC. Rassurez-vous, pour ces experts, il existe de par le monde des PC beaucoup plus intéressant que le vôtre.

3. Les Virus

Le mot virus, est un mot qui signifie poison.

L'origine des virus informatiques remonte années 60, il a été diffusé par un jeu sur des disquettes, mais depuis leur nombre a explosé (presque 100 000 virus répertoriés en 2004) et aujourd'hui, un minimum de 400 nouveaux virus apparaissent chaque mois, et la tendance est à la hausse !

Un virus informatique a comme premier but de se dupliquer sur d'autres PC pour garantir sa survie, et ensuite seulement de nuire plus ou moins gravement au fonctionnement de l'ordinateur infecté.

Les différents types de virus :

- Le virus classique qui s'intègre dans un programme normal
- Les macrovirus s'attaquent à Word, Excel, etc. grâce au VBA de Microsoft.
- Les virus de boot aujourd'hui obsolètes. Pour modifier ou bloquer le démarrage du PC
- Les virus-vers apparus en 2003 Leur mode de propagation est lié au réseau et au Web
- Keylogger Logiciel qui enregistre les frappes au clavier
- Dialer composent un numéro pour connecter votre ordinateur à Internet.

Leurs caractéristiques

- La capacité de se reproduire disquette, CD, téléchargés, mails, pages Web etc...
- La cryptographie à chaque réplication, le virus chiffre vos informations qui deviennent illisibles
- Le polymorphisme c.à.d. la combinaison de plusieurs formes d'attaques
- La furtivité le virus « trompe » le système d'exploitation (et par conséquent les logiciels antivirus) sur l'état des fichiers infectés.

Pour se protéger il faut absolument un logiciel antivirus

Les antivirus sont des logiciels spécialisés capables de détecter les virus, les détruire ou les mettre en quarantaine et en général de réparer les fichiers infectés sans les endommager.

De nombreuses techniques sont utilisées, parmi lesquelles :

- La reconnaissance de séquences d'octets caractéristiques (signatures) d'un virus
- La détection d'instructions suspectes dans le code d'un programme (analyse heuristique) ;
- Renseignements sur les fichiers du système, en vue de détecter des modifications
- La détection d'ordres suspects ;
- La surveillance des lecteurs de support amovible : disquettes, Zip, Cd-rom, ...

4. Les Spywares

L'antivirus ne voit pas tous les programmes malveillants. D'autres menaces existent ils se distinguent par l'absence de système de reproduction caractéristique des virus et peuvent échapper aux antivirus

Un spyware, " ou "logiciel espion", est un programme conçu dans le but de collecter des données personnelles sur ses utilisateurs et de les envoyer à son concepteur ou à un tiers via Internet ou tout autre réseau informatique.

Les types de spywares

- **Les spywares** commerciaux collectent des données sur leurs utilisateurs
- **Les mouchards** idem mais dans la plus totale discrétion
- **Le spyware intégré** (ou interne) inclus dans le code d'un programme
- **Le spyware externalisé** est une application autonome associée avec un logiciel

Une nouvelle tendance concerne les utilisateurs du navigateur Internet Explorer. Certains spywares cherchent à s'installer automatiquement sur le poste au moyen de la technologie ActiveX, lors de la visite de pages Web peu recommandables.

5. Le ransomware

Le ransomware est une des attaques informatiques les plus inquiétantes. C'est un logiciel malveillant, qui bloque l'ordinateur et(ou) prend en otage vos fichiers en les cryptant… et n'en rend le contrôle à leur propriétaire que si celui-ci paye une rançon.

Pour combattre une infection, mettre la main au portemonnaie n'est pas la meilleure solution, l'argent sera certainement encaissé mais vos fichiers risquent de rester inaccessibles… En plus, céder au chantage ne peut qu'encourager les pirates à continuer

6. Les Spams

Constituent des spams les messages adressés sur la base d'une collecte irrégulière de Mails, soit au moyen de moteurs de recherche dans les espaces publics de l'Internet, soit que les adresses aient été cédées sans que les personnes en aient été informées et sans qu'elles aient été mises en mesure des 'y opposer ou d'y

consentir. Une telle collecte est alors déloyale et illicite au sens de l'article 25de la loi du 6 janvier 1978.

Le plus souvent, ces messages n'ont pas d'adresse valide d'expédition ou de "reply to" et l'adresse de désinscription est inexistante ou invalide.

Les spams en chiffres (pour 2004)

- Spams de langue anglaise 84,8 %
- Spams de langue française 7 %
- Autres langues 8,2 %
- Messages à caractère pornographique / Rencontres 42%
- Produits financiers (crédits, remboursement de dettes, prêts, placements, etc.) 40%
- Santé (Viagra, produits pour régimes, hormones, etc.) 12,9%
- Autres 5,3%

7. Les Hoaxs

Les Hoaxes ne contiennent pas de codes malicieux, et représentent surtout un danger humainement parlant. Leur but est de se diffuser le plus largement possible en dupant le plus grand nombre d'internautes avec de fausses informations soit disant très importantes. Ce sont, en effet, ces derniers, croyant aider autrui ou "servir bonne cause", qui le propagent.

Les conséquences :

- La perte de crédibilité de vraies informations diffusées par mail.
- La désinformation des personnes qui vont croire au hoax qui vont donc rediffuser le hoax
- Le remplissage inutile des boîtes mails.
- L'engorgement du réseau au même titre que le pourriel (spam) avec du trafic inutile.
- La circulation de rumeurs fausses sur une personne, une société, une association,

Dans certains cas, de nuire aux internautes en faisant passer un fichier système pour un virus et donc de le faire supprimer.

Pour lutter contre les hoaxs :

Ne transférez jamais un mail sans être 100% sûr de sa véracité, cela fait partie des bons réflexes de l'internaute !

Voici plusieurs sites web dédiés au fact-cheking (vérification des informations) à consulter

- **AFP Factuel** > https://factuel.afp.com/
  La cellule de fact-cheking de l'Agence France Presse (AFP). Vous retrouverez dessus tous les articles vérifiés par l'AFP notamment les plus tendances, comme ceux liés au coronavirus.

- **Rubrique Décodeurs du Monde** > https://www.lemonde.fr/les-decodeurs/
  les journalistes du journal Le Monde traitent des rumeurs et des intox qui circulent sur la Toile pour y distinguer le vrai du faux.

- **Décodex** > https://www.lemonde.fr/verification/
  Le moteur de recherche du Monde : un outil pour vous aider à vérifier les informations qui circulent sur Internet et à décrypter les fausses informations. Le but est d'insérer l'url d'une page web pour détecter si la source est fiable ou non

- **HoaxBuster** > https://www.hoaxbuster.com/
  La plateforme collaborative contre la désinformation : son site internet permet d'identifier les hoax sur la Toile c'est-à-dire les canulars.