Sécurité : pleins feux sur les 10 menaces qui vont peser sur les TIC en 2008

L'éditeur Websense présente sa vision de la sécurité informatique pour l'an prochain… Bilan des courses : les attaques Web vont exploser en 2008 indique l'éditeur. D'après ses prévisions, les jeux olympiques chinois vont être un important vecteur d'infection, comme cela est souvent le cas pour les sujets d'actualité.

Par ailleurs, la popularité toujours grandissante des Macs et des iPhones, va entraîner une hausse des attaques ciblant les utilisateurs des équipements de la pomme. Les internautes qui utilisent les sites de Web 2.0 et les réseaux sociaux vont également devenir des cibles importantes. Le spam va de son côté, connaître « son heure de gloire », avec une hausse du phénomène dans la blogosphère et du les forums, les sites qui hébergent du code malveillant vont également se multiplier.

Pour Dan Hubbard, vp de Websense : *« Aujourd'hui, les attaques évoluent très vite, les cyber-criminels cherchent à éviter la détection, ils dissimulent leurs adresses IP, volent des données, cherchent à contaminer des sites Web légitimes. Les entreprises et les gouvernements doivent absolument comprendre que dorénavant les hackers mènent des attaques ciblées. »*

Les dix menaces qui pèsent sur l'IT

1) Les jeux olympiques

Les cyber-attaques reposent souvent sur des évènements de l'actualité. Les JO de Pékin de 2008 vont donc être une opportunité pour les hackers. Et l'on risque de voir une hausse des tentatives pendant cette période. Les chercheurs des labs de Websense estiment que les attaques DOS vont cibler Pékin et les sites olympiques. Enfin, les sites qui traitent du sport vont certainement être ciblés par les hackers.

2) Le spam malveillant

En 2008, les pourriels vont envahir les blogs, les moteurs de recherche, les forums et les sites Web. Les spammeurs peuvent contaminer des sites Web en laissant des commentaires contenant du spam Web. Pour contaminer un maximum d'internautes, les hackers vont cibler les sites les mieux classés par les moteurs de recherche.

3) L'utilisation des liens comme pourvoyeurs d'attaques

On le sait, le Net est un vaste réseau, composé par des liens et des contenus. Et le Web 2.0 a encore démultiplié les liens. Pour Websense, les hackers vont utiliser ces « liens faibles » et les contenus qui sont compromis. En agissant de la sorte, ils peuvent espérer contaminer un maximum de postes. Les sites les plus vulnérables à ces attaques seront MySpace, Facebook…

4) Augmentation du nombre de sites Web compromis

D'après Websense, le nombre de sites qui vont, sans le savoir, héberger du code malveillant va être

plus important que les nouvelles variantes de codes. Le Web est en passe de devenir le principal vecteur de contamination des postes. Les Hakcers vont utiliser les sites compromis comme les plates-formes de lancement de leurs attaques. Ils vont cibler les sites reconnus et populaires qui occupent une bonne place dans les moteurs de recherche Yahoo et Google…

5) Hausse des attaques ciblées

La popularité grandissante des Mac et des produits de la pomme pourrait bien avoir un impact négatif sur la sécurité des macophiles. Les hackers vont mener des attaques ciblées sur les Mac. Pour Websense, Windows n'est plus le seul OS ciblé par les malfaiteurs de la Toile, l'on peut désormais ajouter à la liste le système MacOSX et l'iPhone

6) Les utilisateurs du Web 2.0 seront des cibles de choix

Cela est déjà le cas en 2007, mais le mouvement va se poursuivre en 2008. Les hackers vont désormais cibler des groupes de personnes, cible leurs intérêts et leurs profiles. Les utilisateurs des sites de Web 2.0 donnent beaucoup d'informations personnelles, ces sites sont considérés comme de véritables mines d'or par les hackers. Pour Websense, il faut donc s'attendre à voir des groupes de personnes appartenant à un réseau 2.0 se faire « profiler » puis attaquer.

7) Amélioration des techniques d'évasion

Le plus important pour un hacker c'est bien de ne pas se faire prendre. Pour cela il dispose déjà de différentes techniques, ils peuvent se cacher derrière des PC Zombies, Spoofer des adresses IP afin d'usurper des identités, attaquer depuis l'étranger… En 2008 ils vont surtout utiliser le Polyscript ou le poly-morphic Javascript. Dans les faits, le code d'une page infectée, est changé à chaque visite. Ce qui rend la détection des menaces plus difficiles. Ils vont ainsi allonger la durée de vie de leurs attaques.

8) Les méthodes de dissimulation des données vont s'améliorer

Websense estime que les hackers vont davantage utiliser la crypto-virologie et mettre au point des méthodes sophistiquées de dissimulation des données volées. Pour Websense, ils vont utiliser la sténographie, dissimuler les donner en utilisant de nouveaux protocoles ou les cachant dans des fichiers multimédias.

9) Renforcement des lois

De nouvelles lois vont permettre d'arrêter d'importants groupes de hackers. En 2007, les attaques à grande échelle se sont attirées les foudres des gouvernements. Websense pense que ce mouvement va se consolider en 2008 et que la collaboration entre les états va permettre des arrestations massives. Pour Websense, beaucoup de grands hackers risquent de tomber en 2008

10) Le Vishing et le spam par voix vont augmenter

Les utilisateurs de terminaux mobiles sont de plus en plus nombreux. Les hackers vont donc chercher à exploiter ce filon avec le vishing et le spam voix. Les tentatives de vishing (phishing sur mobiles) se sont multipliées en 2007, le spam par appels automatisés reste pour l'instant un phénomène assez rare. Pour Websense c'est surtout le vishing qui va exploser en 2008 et cette

méthode associée aux données disponibles sur les réseaux sociaux cela pourrait avoir un effet dévastateur.