Après le phishing, les cyber-criminels attaquent avec l'e-gène

Pourquoi parle-t-on d'économie du piratage sur Internet, n'est-ce pas un peu exagéré ? Je suis certain que non ! Les décideurs semblent encore trop peu préoccupés par la sécurité. Pourtant, une politique globale s'impose en la matière, avec l'ouverture des réseaux et l'arrivée de systèmes d'exploitation et de technologies nouvelles issues de l'Open Source, qui réclament une formation et une expertise accrues. En effet, les tutoriaux sur le Web, aussi bons soient-ils, ne suffisent pas ! En matière de sécurité, les enjeux sont stratégiques, car les attaques des cyber-criminels sont devenues une réalité non seulement technologique, mais aussi économique. Certains cyber-criminels sont payés pour nuire, et utilisent toutes les technologies comme le spam, le phishing [obtention d'informations confidentielles en se faisant passer pour quelqu'un digne de confiance], le pharming [pirater le DSN pour renvoyer un nom de serveur vers l'IP d'un autre site], et bien d'autres. Nouvelle tendance : l'envoi par mail (ou tout autre moyen) d'un code actif qui chiffre tous les documents bureautiques d'un serveur par exemple. Le hacker exige alors une rançon pour envoyer la clé de déchiffrement. Bien entendu, cette rançon sera virée sur un compte protégé? Autre spécificité : les serveurs zombies. La machine de la victime contacte elle-même celle du cyber-criminel, ce qui facilite d'autant le passage des contrôles et des règles de sécurité. *Quelles sont les grandes calamités virales actuelles ?* L'entreprise se doit de surveiller tous les flux Internet et intranet. Et ce d'autant plus que les hackers ne manquent pas d'agilité. Les nouveaux codes malicieux sont en fait des enveloppes vides difficilement détectables qui ne font que leur ouvrir une porte. Autre tendance, les **e-gènes (electronic genes)**, code mobile, qui s'adapte à son environnement et qui peut même intervenir à distance. Il fait fonction d'enveloppe vide et exécute alors la séquence de code reçue pour la rendre active. Avec les rootkits, on passe à un niveau plus subtil encore, en captant les droits administrateur d'une machine. Le hacker dépose sur le poste ou le serveur des programmes portant le même nom que des fonctions système utilisées par une personne ou un programme : ipconfig, notepad, etc. Ce logiciel peut même effectuer la commande demandée pour rester invisible, et effectue en parallèle d'autres commandes : ouverture de port, envoi d'informations, etc. Un cheval de Troie très évolué. Mieux encore, disposant des droits d'administration sur les dossiers système, les hackers utilisent les fonctions du système (DLL). Ils évitent ainsi d'écrire les leurs, et deviennent encore moins détectables. *Alors l'entreprise est condamnée à subir en attendant que cela passe ?* Au sein de l'Esac (*European Antivirus Scientific Center*), avec les équipes du laboratoire de Kaspersky, nous menons une recherche prédictive sur les actions possibles entre codes malicieux, enveloppes, hackers, serveurs zombies, etc. À partir de ces recherches, nous élaborons des scénarios technologiques capables de détecter les différentes étapes d'une attaque de façon dynamique. Alors, il est possible de bloquer l'attaque à différents niveaux. Aujourd'hui, il est même possible de détecter les fausses attaques détournant l'attention et monopolisant les ressources d'un réseau pour ouvrir le chemin à une attaque réelle. Il est important de comprendre la dynamique. Les cyber-criminels modifient leurs attaques et leurs spams en les testant avec les logiciels antiviraux. A chaque mise à jour, ils effectuent de nouveaux tests et reprogramment leurs codes pour franchir les obstacles. Les entreprises doivent donc effectuer les mises à jour en temps au plus vite pour disposer d'une protection optimale. Par ailleurs, il serait souhaitable que tout le monde alerte son éditeur antiviral en cas de problème, même apparemment bénin. L'utilisateur

doit contribuer à sa propre sécurité et à celle de tous. Si personne ne porte plainte, les organisations cyber-criminelles ne sont jamais arrêtées !