Cybercriminalité : de nouveaux risques en 2008

- Informatique - Sécurité Informatique -

Date de mise en ligne : mercredi 6 fÃ©vrier 2008

Spyworld Actu

Dans son rapport 2007, le Club de la sécurité de l'information français esquisse les formes de cybercriminalité qui se sont développées en 2007. Et les risques nouveaux encourus pour cette année.

Alors que les particuliers sont de plus en plus amenés à dévoiler certains éléments personnels, sur leur profession, leurs goûts, ou même leurs convictions politiques, sur des réseaux sociaux, des mondes virtuels ou des jeux de rôles en ligne, les pratiques de cybercriminalité se professionnalisent. C'est pourquoi le Clusif (Club de la sécurité de l'information français), association qui regroupe 600 membres, prestataires de services en sécurité et responsables sécurité au sein d'entreprises, a tiré la sonnette d'alarme, le 17 janvier, en présentant son panorama 2007 de la cybercriminalité.

Attaques dans les mondes virtuels

Première cible pointée par le Clusif : les mondes virtuels, tels que Second Life, et les jeux vidéo sur Internet tels que les jeux de rôles, comme Dofus ou World of Warcraft, qui connaissent un succès grandissant. Ainsi, l'institut d'études Gartner prévoit qu'en 2011, 80% des internautes actifs pourraient avoir une « seconde vie » dans un univers virtuel. Tous ces mondes virtuels sont dotés de leurs propres monnaies, avec un taux de change en euros et en dollars. Résultat, « des marques comme Nike, Adidas ou Toyota, y proposent des produits à acheter en monnaie virtuelle. 1,5 millions de dollars sont échangés chaque jour sur Second Life », souligne François Pagès, chercheur en anti-virus chez le spécialiste de la sécurité informatique McAfee. « L'argent, malheureusement, appelle la malveillance », regrette-t-il, citant plusieurs attaques qui ciblent ces mondes : le vol de mots de passe, pour récupérer l'avatar d'une personne et l'argent qu'il détient, permet à des pirates d'entrer dans cet univers, tandis que des virus et chevaux de Troie, perturbant le fonctionnement du jeu, ont fait leur apparition. Sans compter que ces univers, où le sexe représente une des activités principales, permettent à tout un chacun d'y réaliser des crimes virtuels. Des sociétés se sont même spécialisées dans la vente sur Second Life de positions sexuelles ou d'expériences virtuelles de pédophilie. Autre type d'acte malveillant, la création de faux sites miroirs, copiant le monde virtuel, afin d'attirer les joueurs pour mieux les arnaquer. Le Clusif a même détecté MPack, un outil commercial de piratage, développé par un groupe russe qui a pignon sur rue, sur la Toile.

Détournement des données personnelles sur les réseaux sociaux

Objet d'un véritable phénomène de société, les réseaux sociaux en vogue, tels que MySpace et Facebook, constituent une autre « opportunité de malveillance », souligne Danièle Kaminsky, chercheuse en cybercriminalité à l'université Paul-Verlaine de Metz. « Ils permettent la création de profils détaillés et les individus ne sont pas toujours conscients qu'ils donnent trop d'informations sur eux ». Les entreprises mal intentionnées pourraient y récupérer des informations sur les opinions politiques, les goûts ou la situation professionnelle des membres du réseau, puis utiliser ces données. Ainsi, en juin dernier, Facebook a déposé plainte « contre x » pour tentative d'accès frauduleux à son système informatique. « Il s'agissait probablement d'une société pornographique qui voulait récupérer les données personnelles des inscrits à Facebook », précise Danièle Kaminsky. Autre risque, comme sur les mondes virtuels, que des entreprises malveillantes jouent sur le succès de ces réseaux pour y créer de fausses pages ou des virus afin de piéger les utilisateurs.

Attaques en réputation et espionnage industriel en ligne

Les entreprises constituent aussi des cibles de choix pour les cybercriminels. Avec notamment des cas, de plus en

plus fréquents, d'attaques en réputation via Internet. Telle cette affaire, qui a fait grand bruit en 2007, d'attaques en ligne contre la société antispam Castelcorps. Elle a subi en ligne des attaques en déni de service, puis reçu des virements Paypal en tant que donations à son profit, mais qui provenaient de comptes bancaires pillés par fishing, technique par laquelle des fraudeurs récupèrent auprès de particuliers ou d'entreprises des mots de passe ou numéros de cartes bancaires, en se faisant passer pour des tiers de confiance tels que des banques ou administrations. « Ces donations frauduleuses ont entaché sa réputation, on ne sait pas encore qui en est à l'origine », explique Danièle Kaminsky. Autre type d'attaque, fréquent entre entreprises concurrentes, l'espionnage industriel en ligne. Comme le montrent deux affaires en cours dans la compétition automobile. Dans le cadre de la Formule 1, Mac Laren et Ferrari, ainsi que Mac Laren et Renault F1 se sont ainsi mutuellement accusés d'espionnage, suite à des fuites d'informations stratégiques par des employés. Régulièrement visée en la matière, la Chine, qui a eu droit, en septembre dernier, à des avertissements du gouvernement britannique, mais sans mention d'un mode opératoire particulier. Sauf, en décembre 2007, à propos d'un cheval de Troie implanté à des fins d'espionnage chez Rolls-Royce et Shell.

Post-scriptum :

http://www.echos-judiciaires.com/no...