Social Media Release:

WatchGuard prévient les milieux de l'enseignement : ils sont la cible des cyberdélinquants

Paris (9 novembre 2009) – WatchGuard Technologies

Principaux faits et points nouveaux :

Les menaces liées à l'enseignement devraient augmenter – D'après le Département Américain de la Sécurité Intérieure, 25 % de l'ensemble des failles de sécurité concernent les établissements scolaires. Et bien qu'une majorité d'enseignants estiment que leurs réseaux des campus sont plus sûrs à présent que l'année dernière, WatchGuard prévient que les écoles et les universités continueront d'être victimes d'intrusions et de menaces de toutes sortes.

Pour WatchGuard, les points suivants constituent les principales menaces contre les réseaux, les applications et les données dans les milieux de l'enseignement :

- **Malware & Spyware (logiciels malveillants et espions) –** Les étudiants et les personnels universitaires utilisent le web pour leurs recherches et travaux respectifs mais également pour leurs loisirs. Involontairement, beaucoup d'entre eux sont exposés à des téléchargements ou à des sites web corrompus qui injectent des logiciels nocifs dans leurs ordinateurs. Une fois infectés, leurs ordinateurs sont à la merci des pirates : vol d'identité, perte d'information personnelle, notamment grâce à l'utilisation de logiciels espions ou d'enregistreurs de touches (keyloggers).
- **Virus –** Aujourd'hui, l'e-mail demeure l'un des principaux vecteurs de virus. Malheureusement, selon une enquête récente, 27 % des utilisateurs ne tiennent pas à jour leurs signatures antivirus. Et comme les virus sont toujours à la pointe, ils intègrent désormais des propriétés polymorphes. De fait, les signatures antivirus ne parviendront peut-être pas à elles seules à stopper la prochaine attaque virale.
- **Botnets –** Certaines estimations indiquent qu'entre 15 et 20 % de tous les ordinateurs scolaires et universitaires connectés à Internet, peuvent faire partie d'un botnet (réseau d'ordinateurs zombies). Ainsi « colonisés », les systèmes scolaires et universitaires peuvent être utilisés de façon illégale pour la diffusion de spam, des attaques par déni de service, la fraude au clic, l'usurpation d'identité et bien d'autres.
- **Phishing –**Les escroqueries par phishing (hameçonnage) deviennent plus sophistiquées et sélectives, avec les étudiants en point de mire. Un rapport récent explique que les attaques par phishing via les réseaux sociaux ont un taux de réussite supérieur à 70 %, et précise qu'une majorité d'étudiants y sont exposés.
- **Piratage –** D'après une enquête récente menée auprès de professionnels informatiques dans l'enseignement, 23 % d'entre eux considèrent les pirates issus de la communauté estudiantine comme la plus grave menace pour la sécurité de leurs réseaux. Ce genre de piratage peut viser la modification de notes dans les dossiers ou des méfaits bien pires. En tout cas, il plaide pour une protection accrue des réseaux et des données.
- **Contrôle d'accès –** L'usage des appareils mobiles et du sans fil continue à empoisonner la vie des administrateurs réseaux. Leur principal souci est de contrecarrer l'accès non autorisé aux ressources informatiques scolaires et universitaires. Et comme

l'usage des appareils mobiles croît sans cesse, il sera de plus en plus difficile pour les établissements scolaires de filtrer l'accès à leurs réseaux.

- **Réseaux sociaux –** Les réseaux sociaux, tels que Facebook et MySpace, sont la plus grande menace qui pèse sur les réseaux scolaires et universitaires. En effet, ils sont une plate-forme idéale pour lancer des attaques contre les étudiants et les établissements : spam, virus, malware, phishing et autres. Plus grave encore, l'ingénierie sociale de telles attaques les rend encore plus destructrices, compte tenu du contexte "de confiance" qui règne dans les réseaux sociaux.
- En raison de la nature sensible de l'information sur les étudiants et les établissements (numéros de sécurité sociale, numéros de carte de crédit et autres identifications personnelles), WatchGuard recommande aux écoles et universités de réexaminer périodiquement leurs contrôles, règles et procédures de sécurité informatique.

Mots-clés :
Malware, Spyware, Virus, Botnets, Phishing, Hacking, Piratage, Contrôle d'accès, Réseaux sociaux, WatchGuard

Citations:

- « Compte tenu de l'ampleur des risques d'une part et des gains potentiels des cyberdélinquants d'autre part, les écoles et universités sont devenues l'un des environnements informatique les plus dangereux », déclare Eric Aarrestad, Vice-président de WatchGuard Technologies. « Contrairement aux sociétés et entreprises qui peuvent consacrer de gros moyens à la protection de leurs réseaux et données, les établissements scolaires et universitaires sont plus limités financièrement. Pourtant, ils doivent relever un énorme défi de sécurité en raison de l'interaction dynamique entre leurs étudiants et leurs équipements informatiques ».

À propos de WatchGuard Technologies, Inc.