Etude du Groupe Lexsi sur les réseaux de cybercriminalié

- Informatique - Sécurité Informatique -

Date de mise en ligne : mercredi 1er mars 2006

Spyworld Actu

L'année qui vient de s'écouler a marqué un tournant concernant le nombre de délits commis sur le net. Plusieurs types de menaces sont en recrudescence dont la contrefaçon, l'espionnage économique et les vols et pertes de données.

Cette situation est la conséquence d'un changement radical des motivations des cyberpirates : alors qu'auparavant ils cherchaient la gloire personnelle, ils sont aujourd'hui motivés par l'appât du gain.

Etats-Unis, Russie, Chine, pays du Proche-Orient... le phénomène s'internationalise et fonctionne par réseaux, grâce à un ensemble de personnes maintenus en liaison par des canaux d'informations officieux. Le cybercrime à l'image de la mondialisation, ne connaît pas les frontières et n'épargne ni les individus ni les entreprises.

Les visages de la cybercriminalité

- La contrefaçon

2005 est l'année du déploiement des canaux de distribution en ligne de produits contrefaits. Dans le domaine du luxe comme dans celui des produits pharmaceutiques, la gamme des produits contrefaits s'est largement étendue. Les techniques de promotion se sont criminalisées, notamment via l'utilisation du spam et l'hébergement de sites frauduleux dans les paradis législatifs (Caraïbes, Asie du Sud-est, Europe de l'Est). Les groupes de cybercriminalité se sont internationalisés et ces organisations disposent désormais de ressources financières conséquentes pour assurer leur développement.

- L'espionnage industriel

Les cas d'espionnage industriel se sont multipliés au cours de l'année 2005 et l'utilisation des infiltrations informatiques s'est généralisée. Face à la dématérialisation des documents confidentiels, des groupes spécialisés ont mis à disposition d'entreprises peu scrupuleuses des services de collecte ciblée de documents sensibles via l'utilisation de Chevaux de Troie implantés sur les postes informatiques de dirigeants d'entreprises victimes. A titre d'illustration, aux Etats-Unis, l'ancien directeur IT de Lightwave Microsystems reconnaît avoir volé des sauvegardes informatiques de sa société pour les revendre à un concurrent. Et c'est ce dernier, JDS-Uniphase, qui a prévenu le FBI (1)

- Vol et perte de données

Le vol d'identité est devenu le nouvel eldorado pour ces groupes anglophones, russophones, brésiliens ou chinois. Le développement de marchés noirs où se regroupent pirates et acheteurs a créé un appel d'air sans précédent en 2005. En ne comptabilisant que les cas rendus publics d'intrusions et de vols de bases de données d'entreprises, près de 50 millions d'identités auraient été dérobés sur les 12 derniers mois (identifiants et numéros de cartes bancaires, numéros de sécurité sociale, etc).

Par ailleurs, l'information sensible des entreprises se retrouve, malgré les investissements réguliers en sécurité

informatique, de plus en plus exposée. Il est désormais commun de retrouver des comptes-rendus internes sur des réseaux peer-to-peer ou de trouver des cartographies de systèmes d'information sur des newsgroups ou sur le web. Plusieurs dizaines de millions de postes dans l'entreprise, sont infectées par des logiciels espions qui transfèrent les textes tapés par les victimes sur ces marchés noirs où ces données sont alors vendues pour quelques dollars.

Les canaux de communication de la cybercriminalité

- Forums de discussion " Sites cachés " Sites temporaires

Plus d'informations sur ces canaux très sensibles, disponibles sur interview avec Nicolas Woirhaye, Responsable du pôle Intelligence Economique et expert Cybercriminalité du groupe Lexsi.

Les moyens de lutte Lexsi face à la cybercriminalité

Devant la montée de la cybercriminalité, le groupe Lexsi, 1er cabinet indépendant français de conseil en sécurité des systèmes d'information, a développé un pôle d'intelligence économique. La ligne d'action des consultants vise à détecter les risques transactionnels, les fuites d'informations sensibles ou d'atteinte au SI via l'analyse massive de contenus publics sur Internet tels que des supports Web, newsgroups, mailing lists, réseaux de spams, noms de domaines, Black-lists IP, réseaux Peer to Peer, bases de données techniques.

Des millions de pages, messages et fichiers sont analysés quotidiennement afin de détecter tout signal faible préfigurant une menace potentielle pour une organisation. 10 personnes du groupe Lexsi surveillent l'ensemble des sources d'informations officielles telles que les sites éditeurs et constructeurs ou des sources plus officieuses énumérées ci-dessus (forums de pirates, sites cachés, sites temporaires...).

La cellule est composée d'analystes polyglottes (allemand, anglais, chinois, espagnol, japonais, russe, etc.) spécialisés dans la conduite d'enquêtes sur Internet.

Experts dans la compréhension des réseaux de cybercriminalité, les spécialistes de Lexsi réalisent à la fois des surveillances ciblées et des investigations sectorielles.

Post-scriptum :

http://www.mag-securs.com/article.p...