Reportage: Symantec ouvre les portes de son centre de sécurité (1)

Dublin.- L'organisation du centre *« Security Response »* est très pointilleuse. En aucun cas, les virus ne doivent pouvoir se propager à l'extérieur de l'espace de travail où s'activent des ingénieurs experts.

Ces derniers manipulent, il est vrai, des virus, des vers, des spams et des fichiers-espions parfois très véloces.

La visite du site de Symantec dans la capitale de l'Irlande commence par « la *blue room*« , une salle spécialement conçue pour garantir un accès au réseau Internet plus sécurisé.

« Les ScriptKiddies sont passés de mode » explique Kevin Hogan, senior manager Security Response. *« Le monde de la cybercriminalité est en pleine évolution. Nous sommes passé du niveau des amateurs qui souhaitaient voir leurs noms faire les gros titres de la presse à une génération de hackers qui cherchent souvent des moyens de faire de l'argent »* précise Hogan.

Le centre de Dublin est le plus important du réseau de recherche et d'étude des menaces: il compte 48 ingénieurs qui scrutent et analysent les derniers codes malveillants.

Le centre de sécurité de l'éditeur doit pouvoir fonctionner 24h sur 24H et 7 jours sur 7.

Pour un client le préjudice serait trop important si une menace entraînait l'arrêt de son activité pendant plus de trois heures. En moyenne 200.000 malwares sont traités par les ingénieurs.

Comment cette surveillance constante s'organise? Le principe est simple, les équipes de Symantec suivent l'heure solaire, par exemple, lorsque l'équipe localisée à Tokyo ferme ses locaux, elle passe le relais à l'équipe de Dublin, tout en lui transférant les données qu'elle a traitées, les nouvelles signatures et malwares découvertes.

En moyenne un ingénieur Symantec met **20 minutes** pour analyser une menace et déterminer, s'il s'agit d'une malware ou pas. Ce qui fait qu'après un rapide calcul, un ingénieur de ce centre procède à l'analyse de pas moins de 18 codes malveillants potentiels par jour.

Interrogé sur sa collaboration avec les géants de l'édition comme Microsoft ou IBM et certains concurrents directs comme Mcafee, Hogan précise qu'elle existe, même si elle est limitée.

Le spécialiste de la sécurité explique qu'il est membre de l'OIS, l'Organisation d'Information sur la Sécurité, et que dans ce cadre, il arrive que les éditeurs et les créateurs de logiciels s'échangent des échantillons du code d'un virus.

Cette collaboration s'explique peut-être par le risque que représente les attaques 0day, par exemple les failles découvertes dans la suite bureautique de Microsoft, Office, presque 1 faille par mois dans les File format document, sont très intéressantes pour les Hackers qui connaissent parfaitement la politique de mises à jour de Microsoft et profitent de la fenêtre entre la publication du patch et la découverte d'une faille O day pour lancer des attaques.

Entre 2004 et 2006, les menaces ont changé, les incidents les plus dangereux, ceux de catégorie 3 sont en diminution, Symantec indique que 33 incidents de catégorie 3 ont été signalés en 2004, 5 en 2005 et pour l'instant 0 en 2006.

Il faut dire que l'on est passé d'une guerre contre des vers virulents en 2004 – tandis que les hackers cherchaient à prendre la main sur des machines (de postes) – à des attaques ciblées. Aujourd'hui l'objectif des pirates est clairement lucratif, selon les derniers chiffres de Symantec de juillet 2005:

80% des codes malveillants inscrits au 'top 50' étaient des tentatives de vol de données confidentielles.

545 millions d'escroquerie ont été bloquées en 2004, 1.037 milliard en juin 2005, et 1,45 milliard en décembre 2006.

L'un des meilleurs exemples est l'affaire du couple israélien Haephrati, qui avait concocté un ver « troyen » spécial, placé sur un cd commercial pour infecter une cible bien précise (cf. nos articles).

Les attaques à la mode