Des dizaines d'entreprises étaient la cible des pirates chinois

- Renseignement - International -

Date de mise en ligne : vendredi 15 janvier 2010

Spyworld Actu

L'affaire d'espionnage informatique dénoncée par Google a touché au moins une trentaine d'entreprises américaines. L'attaque durait probablement depuis des mois

L'affaire d'espionnage informatique dénoncée par Google mardi n'embarrasse pas seulement les autorités chinoises, accusées en filigrane d'en être à l'origine. Des dizaines d'entreprises ont été victimes des mêmes agissements, dont l'objectif ne se limitait de loin pas à la surveillance d'une poignée de dissidents. Contrairement au moteur de recherche, les entreprises touchées ont presque toutes choisi de se taire. Google avait déjà révélé mardi que, d'après son enquête, une vingtaine de sociétés avaient été touchées par la même attaque. Selon la société de sécurité VeriSign, il s'agirait plus précisément de 34 entreprises, toutes américaines et actives en Chine.

De l'avis d'un responsable de la sécurité informatique d'une société suisse interrogé par Le Temps mercredi, « l'ampleur de l'attaque et sa sophistication ont de quoi inquiéter toutes les entreprises ayants des intérêts en Chine ». A contrario, le spécialiste des solutions de cryptage pour les télévisions numériques Kudelski ne se montre pas particulièrement troublé par cette affaire. La société vaudoise a ouvert un centre de recherche et développement à Pékin en novembre dernier. « L'importante contribution de nos ingénieurs chinois s'inscrit dans le contexte de notre stratégie globale en matière de sécurité, qui consiste à mettre en place un système diversifié par zones géographiques et par clients », explique le porte-parole, Daniel Herrera. Publicité

Google le dit tout haut

Il est extrêmement rare que des sociétés victimes d'actes de piratage l'admettent publiquement. L'attitude de Google est exceptionnelle à ce titre. « Google a clamé haut et fort ce que nombre d'experts en sécurité disent tout bas depuis des années », a expliqué hier Jeff Moss, le fondateur des conférences Black Hat et DefCon, interrogé par l'AFP. « Ces attaques sont bien conçues et ne sont pas le fait d'une simple bande de pirates », a-t-il ajouté.

Une seule des sociétés touchées, l'éditeur américain de logiciels Adobe, a reconnu en faire partie. C'est par le biais d'une faiblesse dans son lecteur de fichiers Acrobat Reader que les pirates ont pu implanter des logiciels espions dans les systèmes informatiques de leurs cibles. Selon un spécialiste de VeriSign cité par le magazine Wired, toute la sophistication de l'attaque reposait sur l'usage de cette faille inconnue jusqu'ici, notant que les pirates s'étaient montrés « incroyablement bons ».

VeriSign n'a pas donné d'indications sur l'identité des victimes, sauf que certaines figurent parmi ses clients. Des sources anonymes font dire au Washington Post qu'il s'agit notamment de Yahoo, de l'éditeur d'antivirus Symantec, du conglomérat Northrop Grumman et du géant de la chimie Dow Chemical.

« Contrôle parental »

Un cabinet d'avocats de Los Angeles a indiqué avoir été touché de la même manière. L'étude Hoffman & Pancione avait déposé une plainte contre le gouvernement chinois la semaine précédente, exigeant 2,2 milliards de réparations pour le compte de son client, la société Solid Oak Software. L'éditeur du logiciel de contrôle parental Cybersitter affirme que des milliers de lignes de codes ont été volées et utilisées dans un programme similaire de fabrication chinoise.

En observant une partie du code utilisé lors de l'attaque contre Google, VeriSign a établi des liens avec une vague

précédente menée dès juillet 2009. Dans les deux cas, les logiciels espions étaient programmés pour siphonner des données confidentielles vers des serveurs basés à Taïwan. Ceux-ci étaient configurés pour recevoir de très grandes quantités de données, explique VeriSign.

Post-scriptum :

http://www.letemps.ch/Page/Uuid/fb4...