

Extrait du Spyworld Actu

<http://www.spyworld-actu.com/spip.php?article14822>

Une nouvelle campagne de cyberespionnage mondial révélée, Pékin soupçonné

- Informatique - Sécurité Informatique -



Date de mise en ligne : lundi 8 août 2011

Spyworld Actu

Plus de 70 organisations et gouvernements, dont l'ONU et des groupes américains de défense, ont été victimes d'une gigantesque et audacieuse opération de cyberespionnage ces dernières années, a révélé la société McAfee, des experts y voyant l'empreinte de la Chine.

Cette vaste campagne d'espionnage a commencé au moins en juillet 2006 avec une intrusion dans les serveurs informatiques d'une compagnie de construction sud-coréenne et s'est achevée en juin 2011, indique McAfee dans un rapport de 14 pages publié mardi sur un blog de l'entreprise.

Au total, ce sont quelque 72 organisations, dont 49 localisées aux Etats-Unis, qui ont été touchées par cette opération, baptisée "Shady RAT", affirme McAfee, une entreprise de sécurité informatique basée en Californie, qui vend des logiciels antivirus.

Parmi les victimes figurent le secrétariat des Nations unies, un laboratoire du département américain de l'Energie ou encore des dizaines de sociétés de défense américaines. Les gouvernements américain, canadien, sud-coréen, vietnamien, indien et taïwanais ont également été concernés, indique le rapport.

Selon le Washington Post, la campagne de cyberespionnage a également touché l'agence de presse américaine Associated Press (AP).

"Ce que nous avons constaté au cours des cinq à six dernières années constitue un transfert sans précédent de richesses", observe l'auteur du rapport, Dmitri Alperovitch, vice-président de McAfee. "Ce qu'il adviendra de toutes ces données reste une question encore largement ouverte".

M. Alperovitch précise toutefois que "la grande majorité des victimes ont pris des mesures pour mettre un terme à ces intrusions".

Les pirates informatiques cherchaient notamment à mettre la main sur des données sensibles concernant les systèmes de défense américains et de communications par satellite.

Dans son rapport, la société de sécurité n'a pas nommément dénoncé la main de Pékin, mais des experts ont indiqué au Washington Post que la Chine serait derrière l'opération, dans la mesure où de nombreuses cibles identifiées par McAfee avaient un lien avec Taïwan ou le Comité olympique international (CIO) dans les mois qui ont précédé les jeux de Pékin en 2008.

Selon James Lewis, un expert informatique du Centre d'études stratégiques et internationales (CSIS), si les éléments avancés par McAfee ne constituent pas des preuves "concluantes au sens juridique" contre Pékin, la suspicion est grande.

"On peut penser à au moins trois autres vastes programmes (de cyberespionnage) attribués à la Chine qui ont l'air très proches" de celui utilisé pour cette opération, baptisée "mouchard ténébreux", a indiqué M. Lewis à l'AFP. "C'est un mode opératoire que nous avons déjà vu", a-t-il ajouté.

McAfee remarque pour sa part que "pirater les secrétariats des Nations unies ou de l'Association des nations de l'Asie du Sud-Est (Asean) n'est probablement pas le fait d'un groupe seulement intéressé par l'argent".

Une nouvelle campagne de cyberespionnage mondial révélée, Pékin soupçonné

Pékin est régulièrement accusé d'être impliqué dans des cyberattaques. Dernièrement, le géant américain de l'internet Google a affirmé que les comptes de messagerie Gmail de responsables américains, de dissidents chinois, de responsables militaires et de journalistes avaient été piratés depuis la Chine.

McAfee indique que les victimes ont été identifiées à partir des données d'un seul serveur. Pour infiltrer leurs cibles, les pirates envoyaient des courriers électroniques piégés qui, une fois ouverts, installaient des logiciels espions, explique McAfee, en se disant "interloqué par l'audace" de l'attaque.

Pour Dmitri Alperovitch, cette opération de cyberespionnage illustre les menaces de plus en plus fortes qui pèsent sur la toile : "On peut diviser (les entreprises) en deux catégories, dit-il. Celles qui savent qu'elles ont été piratées et celles qui ne le savent pas encore".

Post-scriptum :

<http://www.google.com/hostednews/af...>