Pour Snowden, c'est la Russie qui a piraté la NSA

La négligence de la NSA (National Security Agency) aurait permis à un groupe de hackers sponsorisé par un État d'obtenir certains fichiers de l'agence américaine. Edward Snowden, l'homme à l'origine des révélations sur la surveillance *« Made in NSA »*, pointe la responsabilité russe dans ce dossier.

L'informaticien explique sur Twitter qu'une puissance *« rivale »* des États-Unis peut avoir piraté un serveur que la NSA utilise pour diffuser des malwares dans le cadre d'opérations offensives. Cette pratique est courante dans le renseignement. Par manque de vigilance, des cyber-espions américains pourraient avoir laissé traîner des fichiers binaires sur un serveur piraté. Des hackers tiers auraient ainsi eu la possibilité de s'en emparer et de les mettre en vente aux enchères…

« Pourquoi ils l'ont fait ? Personne ne le sait. Mais je soupçonne qu'il s'agit plus de diplomatie que de renseignement, en rapport avec l'escalade autour du hack du DNC (Democratic National Committee) », précise Snowden. En juin dernier, WikiLeaks a publié des milliers de courriels internes du DNC dont les serveurs ont été piratés. Malgré les revendications d'un hacker présumé roumain (Guccifer 2.0), le parti démocrate US voit la main de la Russie derrière cette opération… Snowden a un point de vue similaire en ce qui concerne la fuite de données appartenant prétendument à la NSA.

Les pirates de l'ombre

Lundi 15 août, un groupe de pirates se faisant appeler Shadow Brokers a publié un échantillon de fichiers qui auraient été dérobés à Equation, un groupe de hackers lié à la NSA. Ces fichiers, dont les plus récents dateraient de 2013, contiennent des vulnérabilités et des outils qualifiés de *« cyber-armes des ennemis »* par les pirates.

Les *« meilleurs fichiers »* ont été mis en vente aux enchères (en bitcoins). Les pirates se targuent aussi d'avoir en leur possession du code inédit, *« meilleur que Stuxnet ».* Il s'agit du ver informatique américain utilisé en 2010 contre les systèmes liés au nucléaire iranien. Les pirates disent aussi avoir des données relatives au piratage de produits réseau d'équipementiers, dont ceux de Cisco. Une affirmation étayée par plusieurs chercheurs qui ont étudie les parties de code mises en ligne par Shadow Brokers et librement accessibles.

> *8) Circumstantial evidence and conventional wisdom indicates Russian responsibility. Here's why that is significant:*
>
> *— Edward Snowden (@Snowden) August 16, 2016*

Un avertissement russe ?

Le choix des enchères par les Shadow Brokers, complété d'un message politique d'opposition aux *« riches élites »*, laisse encore perplexe les spécialistes de la sécurité informatique quant à l'ambition réelle des pirates. Pour Edward Snowden, en revanche, plusieurs pistes mènent vers des pirates financés par un État, la Russie probablement (pays dans lequel l'informaticien s'est exilé). Des pirates dont l'objectif serait de lancer *« un avertissement »* aux États-Unis. Et ce pour plusieurs raisons.

« Quelqu'un peut prouver la responsabilité des États-Unis dans les attaques menées à partir de ce serveur de logiciels malveillants », explique l'ex-consultant de la NSA. Par ailleurs, cette affaire pourrait avoir des *« conséquences politiques internationales importantes »*. En particulier, si une opération offensive menée dans ce cadre cible un allié des États-Unis ou des élections (la campagne présidentielle américaine elle-même divise partisans et contempteurs d'Hillary Clinton et de Donald Trump).

Jusqu'ici, la NSA ne s'est pas prononcée sur la fuite présumée de données. Cisco, en revanche, a déclaré enquêter sur l'incident.

Lire aussi :

Des hackers anonymes auraient piraté les hackers de la NSA

Snowden élabore un étui pour protéger un iPhone des écoutes

La Russie et la Chine auraient décodé les documents Snowden