La NSA aurait mené de nombreuses opérations de piratage

L'affaire **Edward Snowden** n'a décidément pas fini de nous réserver des surprises. Dernière en date, le décompte de 231 cyberopérations offensives effectuées par les services de renseignement américains pendant l'année 2011. Une information dévoilée par le *Washington Post*.

En dehors de ce nombre élevé d'opérations, l'élément le plus explosif est bien la confirmation qu'il s'agit d'actions offensives, c'est-à-dire pour l'essentiel du piratage informatique de sociétés ou gouvernements. Dans l'esprit des patrons du renseignement américain, la cyberguerre semble donc déclarée depuis plusieurs années déjà.

The Washington Post se penche sur le projet **Genie**, d'un budget de 652 millions de dollars, qui consiste en la création, puis la diffusion, de *malwares* sophistiquées. L'objectif est à terme d'infester plusieurs millions d'ordinateurs, routeurs et pare-feu, afin de prendre la main sur un maximum de réseaux, à fins d'espionnage, mais aussi d'atteinte au bon fonctionnement de ces infrastructures informatiques.

Aujourd'hui, 85 000 *malwares* Genie auraient été déployés. Pas sûr que les gouvernements étrangers voient l'invasion de leurs réseaux d'un très bon œil. Auraient été visées des installations situées en Chine, Corée du Nord, Iran et Russie… pour l'essentiel.

Des malwares hypersophistiqués

Quoi qu'il en soit, le marché des *malwares* gouvernementaux est en pleine extension. Le *Tailored Access Operations* (TAO) de la NSA se charge ainsi de créer des outils sur mesure pour infiltrer des réseaux tiers. La pose de mouchards matériels fait également partie des techniques utilisées ici.

Concernant les outils logiciels, leur évolution devrait permettre d'aller encore plus loin, par exemple en détectant des éléments de conversation intéressants (essentiellement via le captage des flux de voix sur IP). Devra-t-on bientôt arracher les micros de nos ordinateurs portables en plus de masquer leur webcam ?

À noter, les technologies employées ici ne sont pas toutes développées en interne. Dans un autre article du *Washington Post*, nous apprenons en effet que la NSA a acheté cette année pour 25 millions de dollars d'outils d'intrusion (et autres *exploits* ou *malwares*).

L'article cite le français **Vupen** comme fournisseur d'outils permettant d'exploiter les failles présentes dans certains logiciels. Le journaliste du *Post* fait d'ailleurs remarquer que Vupen compte prochainement ouvrir des bureaux aux États-Unis… à deux pas du quartier général de la NSA.

« I want you for U.S. [cyber]Army »

Le projet Genie n'est que la première phase d'un plan plus large. Ainsi, la NSA compte mettre en place un système automatisé, nom de code **Turbine**, qui utiliserait les machines infectées, avec comme objectif de mener des attaques massives.

Bref, un *botnet* contrôlé par le gouvernement américain, mais utilisant des machines situées partout dans le monde, au mépris de toute règle de souveraineté nationale.

Le gouvernement américain se défend en rappelant que ces opérations sont lancées contre des pays ennemis (voire en guerre avec les États-Unis) et non pas à des fins économiques. Un argument qui reste un peu faible, en particulier lorsque l'on note que les Russes comme les Européens n'ont visiblement pas été épargnés.

Voir aussi
Quiz Silicon.fr – Fuites de données, petits secrets et grands scandales