# Des hackers anonymes auraient piraté les hackers de la NSA

Un groupe de hackers se faisant appeler Shadow Brokers (les courtiers de l'ombre, en français) a annoncé lundi sur Tumblr avoir piraté des systèmes informatiques utilisés par Equation. Ce dernier n'est autre qu'un groupe de cyber-espions reliés à la NSA (National Security Agency) américaine. Il a été découvert l'an dernier par l'éditeur de solutions de sécurité Kaspersky.

Les membres de Shadow Brokers, de leur côté, ont publié un échantillon des données prétendument dérobées, et certaines sont vendues aux enchères (en bitcoin). *« Combien êtes-vous prêts à payer pour les cyber-armes des ennemis ? »*, interrogent-ils dans leur message (la page sur Tumblr a été supprimée depuis, mais une version en cache est toujours disponible ce mardi 16 août).

## *« Plus fort que Stuxnet »*

Ces fichiers, dont les plus récents dateraient de 2013, contiennent des vulnérabilités et des outils qui auraient été utilisés par Equation. *« Nous vous donnons quelques fichiers d'Equation Group gratuitement… Mais pas tous, nous mettons aux enchères les meilleurs »*, ont indiqué les Shadow Brokers dans un anglais approximatif. Ils se targuent aussi de proposer à la vente du code inédit, *« meilleur que Stuxnet »*. Ce ver informatique conçu par les États-Unis avec le soutien d'Israël, a notamment ciblé les systèmes liés au programme nucléaire iranien en 2010.

## Portes dérobées

Selon un chercheur de l'université de Toronto interrogé par *Wired*, 300 mégaoctets de code livrés par les Shadow Brokers correspondraient effectivement à des opérations menées par la NSA. Mais il est trop tôt pour dire si ce code émane bien d'Equation ou d'un autre groupe de hackers lié à la célèbre agence américaine.

Selon un autre spécialiste, Matt Suiche, cofondateur de la start-up de sécurité Comae Technologies, l'échantillon dérobé montre également que les équipements de sécurité réseau de différents fabricants et marques (dont Cisco Systems, Juniper, Fortigate et l'industriel chinois TOPSE) sont ciblés par Equation.

## Message aux élites

Les Shadow Brokers indiquent qu'une participation aux enchères se fait sans garantie (*« vous pariez, vous prenez les risques »*). Et terminent leur intervention par un message à destination des *« riches élites »*. *« Nous voulons que les riches élites prennent conscience du danger que font peser les cyber-armes, ce message et notre vente aux enchères, sur leur richesse et leur contrôle »*, disent-ils.

Ce message politique et le choix des Shadow Brokers d'en passer par des enchères correspondent

peu à l'image d'un groupe capable de pirater des hackers affiliés à la NSA. Certains spécialistes spéculent même sur le fait que l'opération pourrait être destinée à tromper tous ceux qui seraient prêts à en tirer profit.

**Lire aussi :**

Quand les sous-marins américains piratent les réseaux tiers

La NSA veut exploiter l'Internet des objets, santé incluse

Juniper retire enfin son algorithme made in NSA… sans s'expliquer

**Crédit Photo : Eugene Sergueev-Shutterstock**