Shadow Brokers revient pour vendre des exploits de la NSA

Shadow Brokers a fait les grandes heures de l'été 2016. Petit rappel des faits. Lundi 15 août, un groupe de pirates appelé Shadow Brokers annonçait avoir compromis des systèmes informatiques utilisés par Equation, une organisation réputée proche de la NSA. A l'appui de ses affirmations, ce groupe jusqu'alors inconnu avait posté deux archives sur des sites de partage. La première, en libre accès, renferme 300 Mo de données, où se mêlent des outils et des techniques pour infiltrer des systèmes. Des solutions de sécurité de Cisco, Fortinet et Juniper étaient concernées.

L'autre archive promettait du code inédit, *« meilleur que Stuxnet »*, du nom du ver conçu par les services américains pour infiltrer le nucléaire iranien. Elle était mise aux enchères en réclamant 1 million de bitcoins (soit plus de 500 millions de dollars à l'époque). Une offre mirobolante qui s'apparentait à un pied de nez.

Un site du Zero Net et une liste d'exploits à vendre

Après cet épisode, le groupe Shadow Brokers s'était muré dans le silence en octobre dernier. Mais voilà que la découverte d'un site le remet en selle. Sur ce site, un fichier apparemment signé avec la clé de chiffrement des Shadow Brokers montre que le groupe tente de vendre des exploits à des acheteurs individuels et des fichiers en cache laissent présager d'autres méthodes.

C'est un certain Boceffus Cleetus, qui a découvert le pot aux roses. Dans un message intitulé « *Est-ce que les Shadow Brokers vendent maintenant les outils de la NSA sur ZeroNet ?* », il montre ce nouveau site. ZeroNet est une plateforme d'hébergement utilisant les technologies Blockchain et BitTorrent. Le site en question se nomme theshadowbrokers.bit et propose une liste de services à vendre.

Dans cette liste, on trouve des services avec des noms comme ENVOYTOMATO, EGGBASKET et YELLOWSPIRIT, qui sont rattachés à un type d'attaques, trojan, implant, exploit. Chaque méthode est disponible pour des prix allant de 1 à 100 bitcoins (780 et 78 000 dollars). Il existe une possibilité d'acheter le package entier pour 1000 bitcoins (780 000 dollars). Le site donne la possibilité aux visiteurs de télécharger une sélection de captures d'écran et de fichiers liés à chaque service vendu. Ces fichiers sont signés avec une clé PGP correspondant à la l'empreinte des Shadow Brokers.

Les Shadow Brokers n'ont pas été arrêtés

Sollicité depuis leur silence radio par nos confrères de *Motherboard*, le groupe de pirates vient de répondre brièvement et de manière chiffré au média en ligne. « *The Shadow Brokers n'ont pas été arrêtés* », précise le message en écho à l'arrestation de Hal Martin, consultant externe à la NSA, accusé d'avoir volé des documents et soupçonné d'être derrière le groupe de cybercriminels. Le message sert donc à dédouaner Hal Martin des maux qu'on lui prête et montrer que le groupe continue toujours d'exister.

Sur la vente des exploits, le groupe indique ne pas être « *des criminels irresponsables* », mais plutôt « *des opportunistes* ». Et d'ajouter, « *nous avons donné l'opportunité aux « parties responsables » de faire les choses correctement. Cela n'a pas été le cas. Ce ne sont pas des personnes responsables.* » Difficile de déterminer qui sont ces parties responsables. Toujours est-il que la phrase d'après est sans appel : « *Nous méritons une récompense pour avoir pris des risques, nous demandons donc de l'argent. Le risque n'est pas gratuit*. » Il reste maintenant à savoir si les méthodes d'attaques vendues vont livrer leurs secrets et si d'autres constructeurs sont ciblés.

A lire aussi :

La 2ème taupe de la NSA serait liée aux Shadow Brokers

Shadow Brokers : la NSA coupable de silence et de négligence

Crédit Photo : produktionsbuero TINUS-Shutterstock