Shadow Brokers : d'autres exploits de la NSA contre 22 000 $ mensuels

Ils s'étaient faits discrets pendant quelques mois. Puis, après la tempête médiatique sur le ransomworm WannaCry utilisant des failles de la NSA comprises dans le portefeuille des Shadow Brokers, le groupe de pirates est revenu sur le devant de la scène. Le 16 mai dernier, il a annoncé la création d'un nouveau service, sur abonnement, donnant accès à de nouveaux outils de piratage dérobés et autres données confidentielles.

22 000 dollars en Zcash

A cette époque, le groupe avait fait du teasing sur les nouvelles révélations à attendre au sein du « Monthly Data Dump », nom du club de hack. Dans ce résumé, on trouve des attaques contre les navigateurs web, les routeurs, les terminaux mobiles, Windows 10, le réseau des banques centrales et des prestataires SWIFT. La présentation se termine par des compromissions dans les réseaux des programmes des missiles et armes nucléaires russes, iraniens, chinois et nord-coréen.

Les Shadow Brokers viennent aujourd'hui de donner des détails supplémentaires sur les modalités d'inscription à ce bulletin mensuel d'exploits, ainsi que les conditions tarifaires. Dans un message, il est indiqué que les intéressés devront adresser « *entre le 1er et le 30 juin 100 ZEC* » à une adresse particulière. Le mode de paiement a changé par rapport au Bitcoin demandé préalablement par le groupe de pirates. Zcash (ou ZEC) est une crypto-monnaie plus verrouillée en matière de confidentialité et de traçabilité. Les spécialistes de la sécurité ont constaté ce mouvement depuis la semaine dernière où les Shadow Brokers ont transféré 10,5 bitcoins (soit environ 24 000 dollars) dans une succession de micro-paiements pour éviter d'être tracé. 100 ZEC correspondent à environ 22 000 dollars. Les abonnés recevront ainsi un mail avec un lien leur permettant de télécharger les exploits proposés.

Des doutes sur de nouveaux exploits

Zcash plus sécurisé que bitcoin ? Pas du tout, répond le groupe dans un style inimitable. Pour lui Zcash a des liens avec les gouvernements américain (Darpa, DOD, John Hopkins) et israélien. Malgré cela, il a décidé de tester Zcash ce mois-ci en se gardant la possibilité de changer de mode de paiement pour la livraison de juillet. Le groupe avertit que son club ne s'adresse qu'à des gens de haut niveau en sécurité, des hackers, des éditeurs de sécurité, des OEM ou des gouvernements.

A l'annonce de ce message sur le droit d'entrée au « monthly data dump », les experts en sécurité sont restés sur leur faim et émettent des doutes sur la véracité de la présence d'exploits réellement nouveaux. *« Je pense qu'il n'y a pas de valeur dans leur message en terme de contenus »*, explique Iliasse Sdiqui, l'analyste de l'institut Delma, à nos confrères de *Bleeping Computer*. D'autres considèrent que passer la moitié du message à s'appesantir sur Zcash est un moyen de détourner l'attention sur l'absence de preuves concernant des exploits originaux. Certains seront néanmoins tentés comme au Poker de payer pour voir. L'avenir nous dira si la menace est bien réelle.

A lire aussi :

Shadow Brokers : et maintenant des exploits visant Swift !

Shadow Brokers : des outils de hack pour Solaris dans la nature

Crédit Photo : produktionsbuero TINUS-Shutterstock