Clap de fin pour les Shadow Brokers : pas assez d'acheteurs ou mission terminée ?

Les Shadow Brokers, ce groupe de pirates inconnu jusqu'à août dernier et qui ont divulgué ces derniers mois des outils de piratage probablement dérobés à la NSA américaine, tirent officiellement leur révérence. Dans un court message, ils indiquent être sur le point « *d'effacer leurs comptes* », expliquant que leur activité devient trop risqué et qu'elle n'est pas assez lucrative. Rappelons que les Shadow Brokers ont dévoilé des outils de hacking de premier plan (bien qu'un peu datés), que différents éléments ont permis de rattacher à la NSA (et notamment à son bras armé en matière de hacking, le Tailored Access Operations).

En marge d'une première livraison d'exploits en août (dont certains affectant des firewalls de Cisco, Huawei ou Juniper), puis de la divulgation d'adresses IP présentées comme liées aux opérations de hacking de la NSA, les Shadow Brokers ont tenté de vendre une archive pour une somme colossale (un million de Bitcoins), avant de faire preuve de davantage de modération. Les pirates ont alors mis en vente leurs trouvailles à l'unité sur ZeroNet, une plate-forme d'hébergement de services Blockchain et BitTorrent. Et, selon leurs affirmations, sont toujours prêts à vendre une archive d'exploits Linux et Windows contre 10 000 Bitcoins (environ 7,5 millions d'euros). Pour l'instant, selon les données de Blockchain.info, le compte des Shadow Brokers n'a reçu qu'un peu plus de 10 Bitcoins, répartis dans 72 transactions. Dans son message, le groupe de pirates se dit d'ailleurs « *déçu* » des sommes récoltées. Tout en précisant que son offre reste valable…

Un faux nez de Moscou ?

Mais l'argent était-il la réelle motivation des Shadow Brokers ? L'administration américaine soupçonne en effet les Shadow Brokers de n'être qu'un faux nez des services de renseignement russes. Une création de Moscou dont l'objectif aurait été d'envoyer un message à Washington, afin d'éviter toute escalade trop rapide dans l'affaire des piratages des instances démocrates que l'administration Obama attribue à la Russie. Remarquons d'ailleurs que les Etats-Unis n'ont officiellement pris des mesures de rétorsion et publié des rapports accusateurs qu'en décembre, le président Obama s'étant contenté, selon ses dires, de mettre en garde dans un premier temps son homologue, Vladimir Poutine. A quelques jours de la prise de fonction de Donald Trump, qui ne fait pas mystère de sa volonté de faire repartir les relations avec Moscou sur de nouvelles bases, la mise en sommeil des Shadow Brokers peut être interprétée comme un signe de bonne volonté affichée par Moscou. Même si le groupe de pirates se défend de toute motivation politique…

[A lire aussi : 10 questions pour comprendre l'affaire Shadow Brokers]

Avant de tirer leur révérence, les Shadow Brokers ont mis en ligne une nouvelle archive renfermant 58 outils de hacking pour Windows selon les dires des pirates (61 fichiers en fait, selon des chercheurs ayant ouvert l'archive). Selon les Shadow Brokers, tous ces fichiers sont déjà détectés par le moteur antivirus de Kaspersky (et présentent, de ce fait, peu d'intérêt à la revente). Selon la première analyse du chercheur en sécurité Matt Suiche, ces fichiers, uniquement des implants et non des outils de hacking, sont anciens et présentent peu d'intérêt. Le mot de passe pour accéder à

cette nouvelle archive : « *fucktheworld* ». Un point final 100 % dans le style des Shadow Brokers.

A lire aussi :

Fuite Shadow Brokers : la preuve d'une nouvelle taupe à la NSA ?

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

Une faille Shadow Brokers exploitée par des hackers : Cisco a-t-il bâclé le boulot ?

Crédit photo : produktionsbuero TINUS-Shutterstock