Shadow Brokers : et maintenant des exploits visant Swift !

C'est une véritable bombe que les Shadow Brokers, ce groupe de hackers apparu en août dernier et dévoilant peu à peu des techniques et outils de hacking dérobés à la NSA, viennent de lâcher. Dans une nouvelle livraison postée ce jour, les pirates dévoilent une série d'outils inédits, certains dédiés à Windows, et d'autres voués au réseau interbancaire Swift. « *La partie la plus intéressante de l'archive, car elle renferme les preuves de la plus large infection du réseau Swift à ce jour* », écrit Matt Suiche, un chercheur en sécurité.

Deux outils, JeepFlea_Market et JeepFlea_Powder, semblent dédiés à la compromission du réseau interbancaire mondial, via deux de ses prestataires, EastNets et BCG. L'archive renferme aussi des données précises sur les codes d'accès et sur l'architecture d'EastNets, qui fait office de prestataire de services Swift au Moyen-Orient. Idem pour son partenaire au Vénézuela et au Panama, BCG. D'après les documents mis à disposition, la NSA avait accès à la base de données Oracle renfermant toutes les transactions Swift d'EastNets (avec en prime des milliers de de comptes et de machines d'employés compromis). Au moment où les documents exfiltrés ont été rédigés (2013), BCG semblait par contre ne pas avoir encore été victime des intrusions de la NSA.

« Informations de grande valeur »

« *C'est la première fois qu'autant d'informations est publiée sur la façon dont un Service Bureau Swift fonctionne et sur son architecture interne*, écrit Matt Suiche. *Tout ceci représente des informations de grande valeur.* » S'il est probable que la NSA a ciblé EastNets pour traquer les réseaux de financement du terrorisme, la publication d'autant de données détaillées constitue une sérieuse épine dans le pied pour Swift et ses prestataires (environ 120 prestataires de Service Bureau de Swift sont répartis sur la planète), qui vont probablement devoir faire face à une vague d'attaques.

Rappelons que le réseau interbancaire a récemment été victime d'une autre vague de piratages, ciblant de nombreuses banques sur la planète. Passant par la compromission des postes clients de Swift au sein de banques, cette campagne, dont la Corée du Nord serait responsable selon les Etats-Unis, a notamment abouti au vol de 81 M$ à la banque centrale du Bengladesh, en février 2016. Une somme qui s'est évanouie dans le très opaque circuit des casinos aux Philippines.

Nouvelles révélations dans une semaine ?

En fin de semaine dernière, se disant déçus de la politique menée par Donald Trump, les Shadow Brokers publiaient un premier lot de documents et outils. Y figurait notamment une liste de plus de 900 serveurs appartenant à des universités ou entreprises, serveurs qui auraient été employés par la NSA afin de déployer des malwares, lancer des attaques, voire exfiltrer des données depuis les cibles véritables. Ainsi que des outils de hacking évolués ciblant Solaris, l'OS dont Oracle a hérité avec le rachat de Sun.

Dans leur nouveau message, ce 14 avril, le mystérieux groupe de pirates indique qu'il prévoit de faire de nouvelles révélations, donnant rendez-vous à la semaine prochaine. Au passage, les hackers regrettent de n'avoir trouvé personne pour leur acheter les outils exfiltrés à la NSA –officiellement, leur projet originel. « *Les Shadow Brokers préféreraient se saouler avec McAfee (du nom du fondateur de l'éditeur éponyme, à la réputation sulfureuse, NDLR) sur une île déserte en compagnie de filles canon* », écrivent-ils. Pas sûr que leur humour fasse sourire à Washington ou à Bruxelles, au siège de Swift.

A lire aussi :

Piratage de la banque du Bangladesh : les Etats-Unis incriminent la Corée du Nord

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

Les Shadow Brokers publient les outils de hacking de serveurs de la NSA

Crédit photo : Swift