Cyberattaque à 300 millions de dollars contre les établissements bancaires

Une cyberattaque massive a été menée contre les systèmes informatiques de plusieurs banques. Une centaine d'établissements bancaires répartis dans une trentaine de pays différents – dont la France – auraient été touchés, explique le *New York Times*.

C'est un peu par hasard que la société a découvert ce piratage de grande envergure. Appelée pour intervenir au sein d'une agence bancaire de Kiev (en Ukraine), dont les distributeurs délivraient des billets de façon 'spontanée', la société a découvert que les ordinateurs de la banque étaient infectés par un malware.

300 à 900 millions de dollars détournés

Cette attaque aurait touché plus d'une centaine de banques au cours des deux dernières années. Le malwware **Carbanak** était envoyé par e-mail aux employés des banques, en espérant que l'infection de leur poste de travail permettrait d'accéder aux serveurs internes de l'établissement financier. Des millions de dollars auraient alors été transférés de la Russie, du Japon, de la Suisse, des États-Unis et des Pays-Bas vers des comptes fictifs situés dans d'autres pays.

[Lire aussi notre récent bilan du Forum International de la Cybersécurité]

Selon Kaspersky, il s'agirait ici d'un des vols les plus importants jamais réalisés, avec un total **d'au moins 300 millions de dollars** détournés. La firme a constaté que les vols ne dépassaient pas les 10 millions de dollars, probablement afin de ne pas éveiller les soupçons des banques. Certaines auraient toutefois été piégées plusieurs fois. Aussi la somme dérobée totale pourrait être jusqu'à trois fois supérieure, indique Kaspersky.

Des attaques ciblées et menées avec soin

Un véritable travail de fond, très professionnel, est opéré par les pirates. Ces derniers ne se bornent en effet pas à utiliser un système d'attaque automatisé. Une fois le contrôle pris sur le poste d'un employé, ils captent les saisies effectuées sur l'ordinateur et prennent des copies d'écran, **afin de comprendre les procédures utilisées au sein de l'établissement bancaire**.

[Lire aussi le récent bilan des vols de données dans le monde en 2014]

Une fois ces processus assimilés, diverses méthodes sont employées pour subtiliser de l'argent : transfert de fonds vers un compte externe ; utilisation d'un système de paiement électronique ; programmation d'un distributeur **pour déclencher à distance et à heure fixe l'émission de billets** (qu'un complice vient alors ramasser). Il va sans dire que cette dernière méthode ne permet de subtiliser que de faibles sommes d'argent à la fois. Malheureusement pour les pirates, c'est à cause d'elle que le pot aux roses a été découvert.

Kaspersky Lab a remonté la piste pour découvrir que le groupe à l'origine de cette attaque serait composé **de pirates chinois, européens et russes**. La cybercriminalité n'a décidément pas de frontières. Notez que le 'cybergang' Carbanak serait à l'heure actuelle toujours en activité. Diverses enquêtes sont en cours.

À lire aussi :

Général Marc Watin-Augouard : « progresser dans l'attribution des cyberattaques »
Le vrai coût d'une cyberattaque… selon les assureurs
Cyberattaques : une facture de 4,8 M€ par entreprise en France

Crédit photo : © Oleksiy Mark – Shutterstock