Une attaque « très sophistiquée » cible une centaine de banques – 1 milliard de dollars dérobés…

Une attaque « très sophistiquée » cible une centaine de banques – 1 milliard de dollars dérobés…

Des pirates se sont infiltrés dans les systèmes d'information d'une centaine de banques en 2013, ont dérobé au moins 300 millions de dollars, et agissent encore aujourd'hui, apprend Kaspersky.

C'est l'une des cyberattaques les plus sophistiquées jamais identifiées par Kaspersky. L'éditeur de solutions antivirus russe a dévoilé auprès du New York Times, lundi, les résultats d'une enquête menée depuis 2013 en partenariat avec Interpol et Europol. Conclusions : de 300 millions à 1 milliard de dollars ont été dérobés à une centaine de banques dans trente pays. Active depuis près de deux ans, la cyberattaque a toujours cours.

Pour ces raisons, l'éditeur reste volontairement imprécis sur les informations divulguées, ne fournissant pas, par exemple, le nom des établissements concernés. Les institutions sont basées principalement en Russie, au Japon, aux Etats-Unis et en Suisse. D'après le quotidien américain, JP Morgan Chase figure parmi les cibles.
Ce cybergang basé en Russie, Chine et Ukraine, « a franchi un nouveau cap » dans la méthode employée, souligne Kaspersky, en dérobant des fonds aux banques sans avoir à passer par les clients. L'attaque aurait débuté avec des infections classiques par hameçonnage, quand des employés de banque téléchargeaient malgré eux sur leur poste le malware nommé « Carbanak » – c'est également le nom de ce groupe de pirates.

Observer et imiter les transferts d'argent
Une fois bien installés sur les ordinateurs chargés des transferts de fonds ou de la compatibilité, il peuvent observer discrètement et patiemment les routines des employés et les processus des banques. Les pirates remontent ensuite sur les machines des responsables des transferts et des comptes, où ils installent un outil d'administration à distance (RAT) afin d'en prendre le contrôle et « d'imiter les activités normales ».
Ainsi, les assaillants peuvent créer de faux comptes pour y transférer de l'argent, a priori sans éveiller de soupçons. Si le hameçonnage n'a rien d'exceptionnel en soi, c'est l'aspect méthodique et la patience des pirates que Kaspersky pointe du doigt dans son rapport. De quoi leur avoir évité de s'être fait pincer à ce jour.
Ce qui a déclenché l'enquête remonte à la fin 2013 lorsqu'un distributeur s'est mis à émettre des billets en plein Kiev, en Ukraine. Alertée, la banque concernée a alors missionné Kaspersky. Lequel découvrira assez tôt que cette avarie allait en fait devenir, comparé à l'ampleur de la cyberattaque, le dernier souci de la banque.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

S o u r c e :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-754433-kaspersky-cyber-attaque-banques.html?&svc_mode=M&svc_campaign=NL_ClubicPro_New_17/02/2015&partner=-&svc_position=86524329&svc_misc=-&crmID=639453874_86524329&estat_url=http%3A%2F%2Fpro.clubic.com%2Fit-business%2Fsecurite-et-donnees%2Factualite-754433-kaspersky-cyber-attaque-banques.html