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

Selon le *Wall Street Journal*, c'est la Corée du Nord qui serait à l'origine du piratage de la banque centrale du Bangladesh. Le compte que cette dernière détenait auprès de la Réserve fédérale de New York a été délesté de 81 millions de dollars (75 millions d'euros) en février 2016, suite à une intrusion des pirates sur le réseau interbancaire Swift. Sur la base de sources anonymes proches de l'enquête, le quotidien explique que la justice américaine s'apprête à incriminer des intermédiaires chinois qui auraient aidé Pyongyang à dérober cet argent. Rappelons que les responsables de la fraude avaient planifié de détourner au total près d'un milliard de dollars, mais qu'une grande partie de la somme avait pu être bloquée à temps. Le reste a disparu aux Philippines, où les millions ont été blanchis dans des casinos.

Ce n'est pas la première fois que la main de Pyongyang est désignée dans cette affaire. En mai 2016, l'éditeur Symantec avait déjà relevé les similitudes entre le malware utilisé pour compromettre la banque du Bangladesh – et particulièrement ses postes d'accès à Swift – et le matériel employé lors de l'attaque contre Sony Pictures, fin 2014. Après cette attaque, les Etats-Unis avaient très rapidement pointé la responsabilité de la Corée du Nord. Selon le *New York Times*, les certitudes américaines concernant Sony Pictures s'appuyaient sur l'espionnage de la NSA, qui avait préalablement infiltré les réseaux de Corée du Nord et ainsi pu suivre la cyberattaque en direct.

« Beaucoup d'argent pour la Corée du Nord»

En juin dernier, Mikko Hyppönen, directeur de la recherche de F-Secure et expert mondialement reconnu en cybersécurité, pointait lui aussi la probable responsabilité de Pyongyang dans le détournement de fonds. En raison d'une clef de chiffrement utilisée tant contre Sony que contre la banque du Bangladesh, et permettant d'informer les assaillants des progrès de leurs attaques. Les motivations de l'Etat asiatique selon Mikko Hyppönen ? L'argent tout simplement. « *Les assaillants ont essayé de détourner plus de 900 millions de dollars. C'est beaucoup d'argent, en particulier pour un gouvernement en difficulté comme celui la Corée du Nord* », remarquait alors l'expert, relevant que le budget annuel de ce pays se limite à 4 milliards de dollars. « *C'est la première fois dans l'histoire que nous avons affaire à une attaque d'un Etat-nation dont l'objectif n'est ni l'espionnage, ni le sabotage, mais bien l'argent* », ajoutait-il.

« Si le lien est avéré, cela veut dire qu'un Etat est en train de voler des banques. C'est une grosse affaire », a affirmé Rick Ledgett, le numéro deux de la NSA américaine. Employant le terme banques au pluriel. Rappelons, en effet, que les piratages de banques, via la compromission du réseau Swift, ne se sont pas cantonnés au seul cas bangladais. En décembre dernier,le réseau interbancaire Swift reconnaissait faire face à une menace « *persistante, adaptable et sophistiquée* ». Une menace qui est « *est là pour durer* ».

Plusieurs groupes d'assaillants

Le système interbancaire, utilisé par des milliers de banques et établissements financiers dans le monde pour transférer chaque jour des milliards d'euros, expliquait avoir constaté un nombre « *significatif* » d'attaques depuis la découverte de la fraude au Bangladesh. Et précisait qu'un cinquième de ces tentatives se sont révélées fructueuses pour les assaillants, qui sont parvenus à dérober des fonds. Swift n'a toutefois pas donné d'indications ni sur les noms des banques concernées, ni sur les montants détournés. « *Il y a probablement de multiples groupes de cybercriminels tentant de compromettre les environnements des clients* », expliquait alors Swift.

Si Pyongyang est bien à l'origine du pillage de la banque centrale du Bangladesh – ce qui reste sujet à caution, étant donné la dissémination rapide des malwares et la volonté de la plupart des assaillants de masquer leurs traces en exploitant du matériel développé par d'autres -, il est donc probable que son exemple a, depuis, inspiré d'autres organisations.

A lire aussi :

La fraude sur Swift est bien plus répandue que ce qu'on pensait

Une banque Ukrainienne, nouvelle victime de la fraude sur Swift

Piratage de Swift : la faute à une mise à jour mal maîtrisée ?

Mikko Hypponen : « Le hacking des élections américaines ? Oui, ce sont bien les Russes »