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

La police du Bangladesh et la banque nationale de ce pays, victime d'une fraude qui lui a coûté 81 millions de dollars en février dernier, mettent en cause les techniciens du réseau Swift, utilisé par des milliers de banques et établissements financiers dans le monde pour transférer chaque jour des milliards d'euros. Selon *Reuters*, les enquêteurs estiment que les vulnérabilités exploitées par les pirates pour bâtir leur fraude ont été introduites par les techniciens du réseau international, lorsque ceux-ci ont connecté Swift au premier système de règlement en temps réel interne aux différentes banques du Bangladesh (RTGS), un système mis en place en octobre dernier. « *Ces changements ont accru les risques pour la banque du Bangladesh* », explique à nos confrères Mohammad Shah Alam, le responsable des enquêtes criminelles de la police bangladaise.

LAN, pare-feu, WiFi : les erreurs des techniciens Swift

Ce sont ces erreurs qui auraient facilité l'accès au système Swift de la banque centrale du pays. A distance, un simple mot de passe suffisait pour s'y connecter, souligne la police. « *C'était la responsabilité de Swift de vérifier l'absence de vulnérabilité une fois le système mis en place. Mais cela ne semble pas avoir été fait* », note un responsable de la banque centrale, interrogé par *Reuters*. Selon les enquêteurs, les techniciens de l'organisation belge ont relié les systèmes Swift à RTGS sur le même réseau que celui où sont connectés 5 000 ordinateurs de la banque centrale du Bangladesh accessibles via Internet. Une erreur d'architecture manifeste : ce type d'interconnexion aurait dû passer par un réseau cloisonné.

Les équipes de Swift auraient par ailleurs échoué à installer un pare-feu entre RGTS et les systèmes accédant au réseau international et se sont contentées d'un commutateur rudimentaire et dépassé, inutilisé par la DSI de la banque. Pire encore : au cours de leur intervention, les techniciens ont installé une borne WiFi permettant d'accéder aux ordinateurs Swift, protégés dans une pièce dédiée, depuis d'autres bureaux de la banque centrale. Un accès qu'ils ont évidemment omis de désinstaller après leur passage. Autre erreur que se plaisent à pointer les enquêteurs : la présence d'un port USB actif sur un des systèmes accédant à Swift, une porte d'entrée pour les malwares habituellement désactivée sur des ordinateurs aussi sensibles. « *Nous essayons de déterminer s'il s'agit de négligences ou d'actes intentionnels* », dit Mohammad Shah Alam.

Le malware qui efface les traces

Swift s'est refusé à commenter les affirmations des enquêteurs. Rappelons que, pour mener à bien leur fraude, les hackers sont parvenus à récupérer – par un moyen inconnu à ce jour – les codes d'accès d'utilisateurs légitimes des systèmes Swift au sein de la banque centrale du Bangladesh. Ils ont ensuite employé un malware ciblant spécifiquement un logiciel de l'organisation internationale, afin d'effacer des enregistrements de transferts sortants, d'intercepter des messages entrants confirmant les ordres passés par les hackers ou encore de manipuler des soldes sur des

enregistrements afin de couvrir la fraude.

La coopérative de droit belge (l'acronyme signifie Society for Worldwide Interbank Financial Telecommunication), détenue par 3 000 institutions financières de par le monde, a confirmé être au courant d'un malware ciblant son logiciel Alliance Access et publié une mise à jour de sécurité, dont l'application est obligatoire. Swift a par ailleurs indiqué à ses clients avoir décelé « *un certain nombre de cyber-incidents* », au cours desquels des assaillants ont envoyé des messages frauduleux sur son système « *depuis des systèmes back-office, des PC et des stations de travail connectés par une interface locale au réseau Swift* ». Bref, la banque bangladaise n'est pas la seule à avoir été prise pour cible, même si aucune autre affaire de ce type n'a pour l'instant été rendue publique.

La sortie des enquêteurs bangladais peut être interprétée comme une façon de mettre la pression sur l'organisation internationale. Cette semaine, une réunion doit en effet se tenir à Bale, en Suisse, entre les officiels de la banque centrale du Bangladesh, la réserve fédérale de New York – où était logé le compte bancaire qui a été délesté – et les représentants de Swift afin de discuter du recouvrement des 81 millions dérobés. Rappelons que les cybercriminels à l'origine de cette fraude avaient planifié de détourner au total près d'un milliard d'euros. Les contrôles et sécurités ont permis de bloquer la plupart de ces transferts, mais une partie de la somme s'est évaporée sur des comptes aux Philippines.

A lire aussi :

Cybersécurité : les 5 erreurs fatales de Mossack Fonseca

Ingénierie sociale : les employés sont-ils le maillon faible de la cybersécurité ?