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

Le réseau interbancaire Swift reste sous la menace d'une menace « *persistante, adaptable et sophistiquée* ». Et cette menace « *est là pour durer* ». C'est ce qu'indique l'organisation belge, dans une lettre à ses clients datée du 2 novembre que s'est procuré *Reuters*. Le système, utilisé par des milliers de banques et établissements financiers dans le monde pour transférer chaque jour des milliards d'euros, reste donc soumis à des risques élevés de cyberattaques, environ 10 mois après la découverte d'une fraude qui a permis de dérober 81 millions de dollars à la banque centrale du Bangladesh.

Dans un entretien accordé à *Reuters*, Stephen Gilderdale, le responsable du programme de sécurité des clients de Swift, reconnaît que les utilisateurs du réseau, des banques commerciales et des banques centrales, ont été touchés par un nombre « *significatif* » d'attaques depuis la découverte de la fraude au Bangladesh. Et un cinquième de ces tentatives s'est révélé fructueux pour les cybercriminels, qui sont parvenus à dérober des fonds. Le porte-parole de Swift s'est refusé à donner des indications sur les noms des banques concernées et sur les montants détournés. Jusqu'alors, Swift n'avait reconnu que le piratage de trois de ses utilisateurs depuis février, officiellement sans conséquences financières.

Le support technique des banques pour cible

Selon la lettre de l'organisation belge, les hackers ont perfectionné leurs tactiques depuis la fraude contre la banque centrale du Bangladesh, les cybercriminels visant par exemple les logiciels permettant aux techniciens d'effectuer le support technique sur les machines afin de compromettre les systèmes d'une banque. Et les déclarations de Stephen Gilderdale laissent à penser que plusieurs groupes de hackers tentent de reproduire et adapter le *modus operandi* qui a permis de détourner des dizaines de millions au Bangladesh. « *Il y a probablement de multiples groupes de cybercriminels tentant de compromettre les environnements des clients* », dit le porte-parole de Swift.

Selon un enquêteur interrogé par *Reuters*, au Bangladesh, les pirates auraient bénéficié de complicités en interne. Selon cette source, des employés auraient volontairement facilité l'intrusion des pirates sur le réseau de la banque, afin de leur ménager un accès vers les postes clients accédant au réseau Swift.

Selon la firme anglaise BAE Systems, le détournement dont a été victime la banque centrale du Bangladesh résulte d'un malware ciblant un logiciel client de Swift appelé Access Alliance. Cette souche infectieuse, dénommée evtdiag.exe**,** peut ainsi effacer des enregistrements de transferts sortants, intercepter des messages entrants confirmant les ordres passés par les hackers ou encore manipuler des soldes sur des enregistrements afin de couvrir la fraude. Depuis cet épisode, différentes sources ont fait état de piratages similaires au Vietnam, en Equateur, aux Philippines, en Nouvelle-Zélande ou encore en Ukraine.

A lire aussi :

Une banque Ukrainienne, nouvelle victime de la fraude sur Swift

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

Fraude sur Swift : plusieurs banques sont touchées