Réseau interbancaire : les attaques de pirates informatiques continuent

Le système informatique Swift, qui permet aux établissements financiers de réaliser des millions de transferts chaque jour, est régulièrement hacké...

Par Baudouin Eschapasse
Publié le | Le Point.fr

© DR

Abonnez-vous à partir de 1€

Le réseau interbancaire Swift n'est pas encore tiré d'affaire. Ce système informatique, censé être l'un des plus sécurisés au monde, a encore été la cible il y a quelques jours de hackers. « Trois attaques ont été déjouées depuis la rentrée », a révélé, le 26 septembre, Gottfried Leibbrandt, PDG de la société de droit belge qui administre cette plateforme financière ultrasensible. « Cette nouvelle n'est pas vraiment une surprise », confie Istvan Szabo, spécialiste en cyberprotection chez Balabit IT Security, une société hongroise sollicitée par de nombreux groupes financiers pour verrouiller leurs systèmes d'information.

Basée à La Hulpe, près de Bruxelles, l'entreprise Swift (dont l'acronyme signifie Society for Worldwide Interbank Financial Telecommunication) est détenue et contrôlée par ses adhérents : 10 000 institutions financières réparties dans plus de 150 pays, parmi lesquels figurent les plus grosses banques mondiales. Le réseau qui porte, lui aussi, le nom de Swift, opérationnel depuis 1977, a beau être prétendument fermé pour protéger les milliards de dollars qui y transitent chaque jour, le système est l'objet de cyberbraquages réguliers depuis un an.

Des braquages « sans armes ni violence »

En février dernier, des pirates informatiques étaient ainsi parvenus à s'introduire sur le réseau et

avaient tenté de détourner un milliard de dollars à la Banque du Bangladesh. Mais, en raison d'une erreur de saisie de leur part, ils n'étaient parvenus à dérober « que » 81 millions de dollars. « Même si toutes les attaques n'ont pas été rendues publiques, au moins cinq autres cyberbraquages se sont produits contre des établissements financiers, via le réseau Swift », témoigne Vincent Hinderer, expert en sécurité informatique au sein du cabinet Lexsi, racheté au printemps par la division cyberdéfense du groupe Orange.

Parmi les victimes figurent une banque asiatique (la Sonali Bank), qui s'est fait dérober 250 000 dollars d'un simple clic dès 2013, mais aussi Banco del Austro, une banque équatorienne, qui a vu s'évaporer 12,2 millions de dollars en janvier 2015. L'affaire n'a filtré dans la presse qu'un an plus tard. En décembre dernier, plusieurs banques de Singapour, australiennes, japonaises, italiennes et américaines ont également été visées. La Tiên Phong Bank, une banque vietnamienne par laquelle transitaient les ordres de virement frauduleux, assure que cette tentative de détournement a été déjouée. Cependant, les 12 millions de dollars qui ont été prélevés, ici et là, pendant quelques secondes puis qui ont circulé de l'un à l'autre de ces établissements n'ont pas tous été retrouvés. Une banque ukrainienne et une autre philippine ont également été pillées. Mais aucune d'entre elles ne veut témoigner.

Un expert informatique, Simon Choi, du cabinet sud-coréen Hauri, a établi en mai dernier une carte recensant toutes les attaques (ou tentatives d'attaque) du réseau Swift rendues publiques à travers la planète. Pour Istvan Szabo (BalaBit), cette carte est incomplète, car « les cybercriminels utilisent des comptes utilisateurs qui bénéficient d'un haut niveau de privilèges, ce qui leur permet de réaliser des actions importantes tout en couvrant facilement leurs traces ».

La multiplication des « hold-up » numériques inquiète... jusqu'à la Réserve fédérale américaine. Cela a obligé Swift à renforcer la sécurité de ses systèmes, « lesquels n'ont pas été directement compromis par les pirates », insiste, sous le couvert de l'anonymat, un ingénieur ayant eu à intervenir sur ce réseau. « À ce stade, ce sont les institutions membres qui ont été attaquées », souligne la même source. Mais le résultat a été le même et des sommes importantes ont ainsi été volées.

« Globalement, les réseaux bancaires restent bien protégés, mais l'ingéniosité des pirates oblige les acteurs du marché à régulièrement se réinventer », confie Gerome Billois, expert en cybersécurité au cabinet Wavestone, à quelques jours du début des Assises de la sécurité et des systèmes d'information, qui se tiendront, comme chaque année, à Monaco du 5 au 8 octobre.

Inquiétudes sur la planète finance

Les dernières tentatives d'intrusion dont le réseau Swift a fait l'objet étaient au centre de toutes les conversations au Sibos, la plus importante convention financière de la planète qui s'est terminée le 29 septembre à Genève. L'intervention de Gottfried Leibbrandt n'y est pas passée inaperçue. D'autant moins que le PDG de Swift a fait plusieurs confidences troublantes. Il a ainsi évoqué un appel téléphonique reçu il y a quelques mois. « Une de nos banques avait été alertée sur des transactions bizarres par l'un de ses correspondants chargés des compensations. Le correspondant a

remarqué que le bénéficiaire final de ces opérations, un compte mule, apparaissait dans des transactions avec une autre banque que nous avons contactée et nous avons constaté que celle-ci avait également été piratée », a-t-il déclaré. Une enquête a montré que la banque en question avait elle-même été hackée et que les rapports de paiement avaient été trafiqués.

Gottfried Leibbrandt a également fait état d'une autre attaque ayant visé une entreprise pourtant « équipée du dernier antivirus et (qui) avait mis à jour (son) logiciel avec le dernier patch de sécurité (fourni par Swift en juillet). Les alertes de l'antivirus et du dernier patch de sécurité ont empêché d'autres fraudes contre la banque ».

Sécurité renforcée

Le PDG de Swift veut croire que les mesures prises depuis la fin du mois d'août vont empêcher les pirates informatiques de continuer leurs méfaits. « Les banques sécurisent désormais leurs environnements en utilisant l'authentification multifactorielle, impliquant divers outils », confie Thierry Karsenti, vice-président de la filiale européenne de Check Point qui sécurise les réseaux de plusieurs grandes banques occidentales. Mais il faut désormais faire un gros travail de formation auprès des milliers d'autres banques qui font partie du réseau Swift. « L'enjeu est simple : il faut que tous les salariés intègrent les règles de base d'une hygiène numérique », énonce Benoît Grunenwald, directeur commercial et marketing de l'éditeur slovaque ESET, lui aussi très actif sur ce créneau.

Swift a ainsi écrit à ses clients pour leur signifier qu'ils devront se conformer à 16 normes de sécurité contraignantes, à partir du 1er janvier 2018. Dans 10 mois, le réseau procédera à des vérifications pour s'assurer que tous ont respecté les consignes. De fait, c'est par des défaillances ou maladresses de banques « branchées » sur la plateforme Swift que certaines attaques ont réussi.

« Les attaques ciblant les établissements financiers vont se poursuivre, et elles seront de plus en plus sophistiquées », pronostiquait Gottfried Leibbrandt en début de semaine. « La cybersécurité va devenir un enjeu majeur pour toutes les entreprises qui fonctionnent en réseau », complète David Sportes, cofondateur du cabinet de conseil Harmonie, spécialisé en sécurité numérique. David Sportes estime ainsi que les grandes compagnies d'assurance seront ainsi les prochaines cibles des pirates informatiques.