Tirer les leçons de « l'affaire Swift »

Par Hervé Postic

Zubair Bin Huda se souviendra longtemps du 5 février 2016. Pour ce directeur de la Banque du Bangladesh (la banque centrale), ce jour restera celui où 81 millions de dollars ont été volés à son employeur à la suite d'une attaque de *malware* qui a modifié le fonctionnement de sa station Swift. Révélée progressivement, l'affaire est devenue l'affaire Swift fin avril quand BAE Systems a dévoilé le résultat de ses investigations (1). Pour la presse non réellement spécialisée, l'affaire était entendue, du moins dans les titres : *Swift victime de cyberattaques, La cyberintrusion du réseau de messagerie bancaire international Swift fait frémir la communauté internationale.* Lire le compte-rendu de BAE et en tirer quelques conclusions permet de distinguer les responsabilités multiples et de rappeler quelques règles de bon sens.

Où est le maillon faible ?

Si, comme la coopérative le rappelait dès le 25 avril, le réseau Swift à proprement parler n'a pas été victime d'intrusion, c'est le logiciel d'accès aux systèmes de messagerie de la coopérative interbancaire, Swift Alliance Access (SAA), qui a été détourné avec succès. Les malfrats ont réussi à remplacer des programmes exécutables qui font partie de SAA, peut-être tout simplement grâce à une complicité au sein de la banque ayant les droits d'accès à l'ordinateur qui héberge SAA. Ces programmes malicieux ont été modifiés par des grands connaisseurs de la solution et ont permis de créer et de modifier des messages émis et de faire les modifications afférentes dans les journaux de transmission, en détournant les nombreux contrôles opérés par les différents programmes composant la SAA.
Depuis cette première attaque, d'autres cas similaires ont été dévoilés qui faisaient dire à Swift le 13 mai dernier que le premier cas fait partie d'un ensemble important d'attaques très pointues (2). Les malfrats ont pu intervenir car ils ont eu accès aux ordinateurs sur lesquels sont installés les logiciels composant SAA et, très certainement, à des noms d'utilisateurs et mots de passe permettant d'y intervenir.

Swift 4 Corporates menacé ?

Les entreprises utilisatrices de Swift peuvent être réparties en deux familles : celles qui ont recours à un service bureau (80 % en France) et celles qui utilisent Swift Alliance Light. Dans aucun de ces deux cas elles n'ont de personnes directement utilisatrices de la SAA, qui est hébergée par le service bureau ou par Swift. Les entreprises utilisent des liens sécurisés entre leurs plates-formes de paiement et les solutions d'accès aux systèmes de messagerie de Swift (RAHA, LAU). De plus, les systèmes attaqués étant toujours ceux qui ont le plus d'utilisateurs, dans le cas d'espèce, les messages frauduleux ont été émis par FIN et non par FileAct (3), qui est le principal système de messagerie utilisé par les entreprises en France.

Faut-il pour autant s'estimer à l'abri ? Certes non, car la fraude protéiforme dont les trésoreries sont l'objet pourrait bien prendre aussi ce visage. Profitons-en pour rappeler un certain nombre de règles et pour donner quelques idées permettant d'améliorer la sécurité globale des paiements émis par les entreprises.

La première de ces recommandations relève du bon sens et s'applique à tous en tout temps et tout lieu : la gestion des mots de passe et droits d'accès doit être renforcée et plus personne ne doit tolérer des pratiques jadis courantes : « prêt » de mots de passe, utilisateurs ayant quitté la société toujours actifs dans les systèmes (quand ce n'est pas dans les pouvoirs bancaires), clés ou cartes de signature des paiements « partagées » par souci d'économie ou par réflexion insuffisante sur

(1) http://baesystemsai.blogspot.fr/2016/04/two-bytes-to-951m.html
(2) https://www.swift.com/insights/press-releases/swift-customer-communication_customer-security-issues
(3) FIN est le système de messagerie historique de Swift, opérationnel depuis 1977 et avec lequel 12000 banques échangent des messages de paiement internationaux et/ou de gros montants, des confirmations d'opérations de marché et des messages relatifs aux opérations sur titres. FileAct est un système opérationnel depuis le début des années 2000, avec 4000 utilisateurs dans des groupes d'abonnés fermés.

les procédures de signature (le signataire refuse de déléguer sa signature mais prête sa clé de signature à son assistante).

La seconde tient en cinq caractères : 3SKey. Si cette solution de signature personnelle est de plus en plus utilisée par les clients d'Ebics-TS (4), elle est encore insuffisamment adoptée par les clients de Swift. Or, elle assure un scellement et une signature des ordres au-delà du réseau Swift, entre le signataire et l'application de la banque qui va vérifier le sceau et les droits du signataire. 3SKey, ou d'autres solutions qui assurent la même fonction, ajoutent à la sécurité incombant au réseau une sécurité que seul le détenteur conjoint de l'objet (clé, care à puce, téléphone dans le cas de mot de passe à usage unique) et du code d'accès peut activer. Elle permet de pallier une éventuelle brèche ouverte dans les systèmes du tiers, service bureau, hébergeur ou Swift lui-même (5).

Troisième recommandation réservée aux utilisateurs de Swift : la migration de FIN vers FileAct devrait être réalisée. Non seulement parce que l'attaque a été réalisée via FIN, mais surtout parce que la signature personnelle telle qu'elle existe aujourd'hui (3SKey) ne peut s'appliquer qu'aux échanges via FileAct. Beaucoup de banques proposent aujourd'hui de recevoir les virements de trésorerie et internationaux indifféremment par FIN ou FileAct.

Quatrième recommandation réservée aux banques qui n'ont pas encore décidé de proposer 3SKey à leurs clients FileAct : ne tardez plus, cette solution apporte un niveau de sécurité qui vous garantit la provenance des ordres à exécuter.
Les attaques continueront, des banques verront leur nom jeté en pâture comme des trésoriers victimes de la fraude au président ont pu voir le nom de leur entreprise s'étaler dans les pages de faits divers des quotidiens. L'informatisation a été pendant des années un des facteurs de sécurisation, elle peut être aujourd'hui le maillon le plus faible de la chaîne si les clés sont laissées à la portée de n'importe quel passant. Les règles les plus élémentaires doivent être rappelées, martelées et mises en œuvre inlassablement.

Des investissements pas toujours jugés prioritaires

La lutte contre les cyberattaques fait l'objet de développements dans le rapport « Evaluation des risques du système financier français » publié en juin par la Banque de France.

Les auteurs y signalent les initiatives prises par la Commission européenne (directive *network and information security* adoptée en mai), la France, la Banque centrale européenne (enquête auprès de 110 banques européennes au printemps 2015, missions sur la cybersécurité dans des banques, collecte des incidents de sécurité qui sera étendue à tous les établissements significatifs l'année prochaine...) ou des banques centrales nationales.

Ils rappellent aussi, sommairement, ce que doit être un dispositif de sécurité informatique et notent : « *Surtout, la sensibilisation des dirigeants est primordiale afin qu'ils intègrent ces risques dans la stratégie d'entreprise et allouent les budgets nécessaires à la mise en place de dispositifs visant à réduire les risques liés à la cybersécurité (...) Il devient par conséquent urgent que les dirigeants de banques prennent la pleine mesure des risques en matière de cybersécurité et que les dispositifs de sécurité soient renforcés.* »

Cette mise en garde voilée aux dirigeants d'établissements financiers a été encore plus explicite dans la bouche de Bernard Delas, le vice-président de l'Autorité de contrôle prudentiel et de résolution, cité par *Le Monde*, qui expliquait le 16 juin que les parades « *exigent de lourds investissements, qui ne sont pas toujours jugés prioritaires* » et notait que « *les nécessaires investissements de sécurité sont largement sous-estimés* ».

A propos de Swift et de la perte subie par la Banque du Bangladesh, le rapport de la Banque de France estime que l'incident « *met en évidence plusieurs points de vigilance* » : i) la sous-estimation des risques par les dirigeants ii) un système d'information insuffisamment sécurisé, en particulier une ségrégation insuffisante des environnements et une gestion inadéquate des droits d'accès des administrateurs des systèmes, et iii) des dispositifs de contrôle défaillants.

A.B

(4) Ebics-TS est un protocole de télétransmission sécurisé banque-entreprise très répandu en France incluant la signature personnelle des fichiers de paiement transmis.
(5) On regardera à ce sujet avec un intérêt renouvelé la présentation faite avec Chérifa Hemadou aux Journées de l'AFTE le 15 novembre 2011.