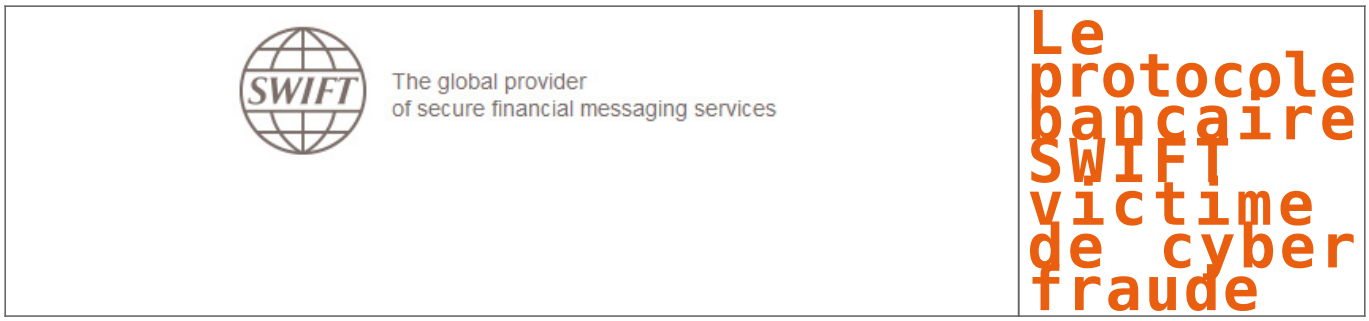
Le protocole bancaire SWIFT victime de cyber fraude



Suite à la récente cyber attaque la Banque du Bangladesh, l'organisme SWIFT vient de reconnaître que son logiciel a été utilisé pour cacher des preuves de transferts frauduleux.Par Aimee Chanthadavong, ZDNet.com | Mardi 26 Avril 2016

SWIFT (Society for Worldwide Interbank Financial Telecommunication), le réseau financier mondial que les banques utilisent pour transférer des milliards de dollars chaque jour, vient d'avertir ses clients « d'un certain nombre de récents incidents de cybersécurité » sur son réseau : les attaquants ont utilisé son système pour envoyer des messages frauduleux.

Cette révélation intervient alors que les autorités du Bangladesh continuent leur enquête sur le vol de 81 millions de dollars en février dernier. Le transfert litigieux a transité d'un compte de la Banque du Bangladesh vers la New York Federal Reserve Bank. Un des enquêteurs, Mohammad Shah Alam, du Forensic Training Institute du Bangladesh, a déclaré à Reuters que la Banque du Bangladesh était une cible facile pour les cybercriminels car il n'y avait pas de pare-feu et que par ailleurs des commutateurs d'entrée de gamme étaient utilisés pour connecter les systèmes informatiques de la banque à SWIFT.

5 paiements frauduleux sur 35 ont été autorisés

Les chercheurs en cyber-sécurité qui travaillent sur ce hold-up ont expliqué le mois dernier qu'un logiciel malveillant avait été installé sur les systèmes informatiques de la Banque du Bangladesh. Ce malware a permis aux attaquants de se dissimuler avant de prendre l'argent. Un rapport interne de la Banque du Bangladesh mentionne que la Réserve Fédérale a été négligente : elle a validé les fausses transactions. Le rapport parle de «faute majeure». Il indique également que 5 paiements frauduleux sur 35 ont été autorisés (pour un total de 951 millions de dollars), et que des entités situées aux Philippines et au Sri Lanka ont reçu une partie des fonds volés. Et c'est une faute d'orthographe commise par les cybercriminels qui a empêché 20 autres millions de dollars de disparaître en plus des comptes de la Banque du Bangladesh.

Ce vol a provoqué la démission du responsable de la Banque du Bangladesh, Atiur Rahman, 64 ans. Il n'avait pas jugé bon d'informer le ministre des finances du Bangladesh, A M A Muhith, de l'incident. Ce dernier avait appris cet évènement dans la presse étrangère.

SWIFT a reconnu que l'attaque incluait la modification des logiciels SWIFT sur les ordinateurs de la banque pour dissimuler les preuves de transferts frauduleux. « SWIFT est au courant d'un certain nombre d'incidents de cyber récents dans lesquels des personnes malveillantes dans l'entreprise, ou des pirates externes, ont réussi à envoyer des messages SWIFT depuis les back-offices, PC ou postes de travail des institutions financières connectées au réseau SWIFT » avertit l'organisme dans une message d'avertissement à ses clients.

L'avertissement, émit par SWIFT via une alerte confidentielle envoyée sur son réseau lundi, ne donne ni le nom des victimes ou le montant des sommes dérobées. SWIFT a également publié une mise à jour de sécurité pour le logiciel que les banques utilisent pour accéder à son réseau.

SWIFT : 3 000 institutions financières, 11 000 banques

Cette mise à jour doit sécuriser son système vis à vis du malware que les chercheurs de BAE Systems soupçonnent avoir été utilisé dans le hold-up de la Banque du Bangladesh. Les preuves collectées par BAE suggèrent que les pirates ont manipulé le logiciel Alliance Access de SWIFT, que les banques utilisent pour s'interfacer avec la plate-forme de messagerie de SWIFT, afin de brouiller les pistes. BAE a cependant mentionné ne pas pouvoir expliquer comment les commandes frauduleuses ont été créés et poussés à travers le système. SWIFT a cependant fourni des éléments sur la façon dont tout cela est arrivé. L'organisme explique que le modus operandi était similaire dans toutes les opérations frauduleuses. Les agresseurs ont obtenu des informations d'identification valides et ont pu créer et approuver des messages SWIFT.

SWIFT (Society for Worldwide Interbank Financial Telecommunication) est une coopérative détenue par 3 000 institutions financières. Sa plate-forme de messagerie est utilisé par 11 000 banques et autres institutions à travers le monde et est considéré comme un pilier du système financier mondial. SWIFT a dit aux clients que la mise à jour de sécurité doit être installée avant le 12 mai… [Lire la suite]

Réagissez à cet article

Source : *Le protocole bancaire SWIFT victime de cyber fraude – ZDNet*