الجمهورية الجزائرية الديمقراطية الشعبية
REPUBLIQUE ALGERIENNE DEMOCRATIQUE ET POPULAIRE
وزارة المالية
MINISTERE DES FINANCES
CTRF
CELLULE DE TRAITEMENT DU RENSEIGNEMENT FINANCIER
خلية معالجة الإستعلام المالي
خ ا م

LETTRE D'INFORMATION : BON A SAVOIR (N°28)

Swift : Le réseau banquier international fait face à une grosse attaque de hackers

Selon une lettre que Swift s'apprête à envoyer vendredi à ses utilisateurs, les méthodes de ces hackers présentent des similitudes avec l'attaque qui avait permis en février à des malfaiteurs de dérober 81 millions de dollars sur un compte de la Banque centrale du Bangladesh auprès de la Réserve fédérale à New York.

Le FBI soupçonne que les malfaiteurs de février avaient bénéficié de complicités internes, avait affirmé mardi le Wall Street Journal.

Le même jour, des hauts représentants de la Réserve fédérale de New York, de la Banque du Bangladesh et du système de paiement international Swift, se sont rencontrés à Bâle, en Suisse, pour discuter de cette fraude cybernétique.

L'attaque menée contre Swift -Society for Worldwide Interbank Financial Telecommunication- montre une véritable tentative pour obtenir un accès à ce système indispensable pour le fonctionnement du monde financier international, selon le texte que s'apprête à publier Swift, cité par le New York Times et le Wall Street Journal.

Cette fois-ci, l'attaque visait une banque commerciale dont elle ne donne pas le nom, et dont les malfaiteurs ont réussi à s'approprier les codes pour envoyer des messages au nom de la banque.

En février, des messages semblant provenir de la Banque du Bangladesh avaient ordonné le transfert vers différents comptes aux Philippines de 81 millions de dollars.

Les méthodes utilisées par les hackers dans ces deux cas « montrent clairement une connaissance approfondie et sophistiquée des opérations de ce type dans les banques visées », selon la lettre de Swift, toujours citée par les journaux. Mai 13, 2016.

Source: RTLInternational

Liens : http://www.koldanews.com/2016/05/13/swift-le-reseau-banquier-international-fait-face-a-une-grosse-attaque-de-hackers-a539130.html

Paiements internationaux : Swift prépare sa mue 2.0

La messagerie bancaire sécurisée s'engage à effectuer les transferts d'argent internationaux en un jour d'ici un an. 21 banques expérimentent de nouveaux processus d'échanges entre elles.

Le système de messagerie bancaire sécurisée Swift prend le taureau par les cornes. La coopérative de banques et d'institutions financières, dont l'infrastructure est utilisée par près de 11.000 membres dans quelque 200 pays pour garantir l'échange de données financières réalisé lors d'un paiement ou d'un achat de titres, a décidé de « *réinventer les paiements internationaux sur la base de nouveaux standards* ». Elle a lancé pour ce faire en décembre

dernier un plan baptisé « Global payment innovation initiative » auquel se sont ralliées 45 banques fin janvier.
Sur ces 45 établissements qui couvrent 67 % des échanges transfrontaliers traités par Swift, 21 lancent un pilote qui doit d'ici l'automne faire la preuve que le réseau de banques correspondantes de la messagerie, vieux de près de 45 ans , reste pertinent et compétitif face à de nouveaux entrants.
Les chiffres clefs
45 institutions financières se sont engagées à adopter de nouvelles règles d'échanges à partir de 2017.
67% des paiements internationaux traités par Swift devraient alors être réalisés en un jour.
En pratique, les établissements participants s'engagent à ce qu'un transfert d'argent par une grande entreprise cliente, fait au sein du réseau international des banques pilotes, soit crédité en un seul jour ouvré. C'est en effet là que le bât blesse : une opération qui transite via Swift prend aujourd'hui au minimum trois jours et le délai peut aller jusqu'à neuf jours selon la complexité du transfert. Ce, sans que le client ne soit informé sur l'état d'avancement de l'opération ni assuré du délai exact pour que l'argent transféré le soit réellement, ni qu'il soit sûr du coût précis de l'opération. Ces incertitudes sont devenues incompréhensibles voire intolérables dans un monde où l'instantanéité est devenue la norme. Elles font d'ailleurs le succès de nouveaux acteurs comme Transferwise ou Paypal.

Plan stratégique

« La messagerie Swift n'est pas du tout en cause, ce sont les pratiques des banques du réseau en matière de transfert qui doivent être réinventées », souligne Thierry Chilosi, responsable Market initiatives chez Swift. Autrement dit le fonctionnement du réseau de banques correspondantes chargées d'acheminer le transfert doit être sérieusement dépoussiéré et c'est ce à quoi se sont engagés les 21 établissements du pilote via un corpus de nouveaux accords de services multilatéraux proposés par Swift. Cet ensemble de règles devra être validé à la conférence annuelle Sibos organisée par la messagerie internationale à Genève fin septembre, avant d'être étendu aux 45 banques volontaires en 2017.
En parallèle Swift va lancer en mai une réflexion afin de définir une stratégie à cinq ans sur la manière dont la messagerie peut intégrer de nouvelles technologies afin d'améliorer la qualité et le coût de son service. Cela étant, Swift ne craint pas d'être balayé par des innovations comme la Blockchain qui permet de valider des transactions sans passer par un tiers de confiance. « *La technologie ne suffit pas, elle permet d'adresser la question du transfert lui-même mais pas tout ce qui tourne autour et notamment les sujets liés à la lutte contre le blanchiment* », prévient Stanley Wachs, directeur international de l'innovation dans les paiements chez Swift. 14/03/16

Liens : http://www.lesechos.fr/finance-marches/banque-assurances/021765608971-paiements-internationaux-swift-prepare-sa-mue-20-1206874.php

Conséquence de l'interruption du réseau SWIFT en Iran

Répondant aux injonctions européennes dans le cadre des sanctions internationales relatives à la conduite de la recherche d'armement nucléaire, la société SWIFT bloque depuis mi-mars les transactions en provenance ou en direction de la plupart des institutions financières iraniennes. Tony Wicks, expert en Blanchiment d'Argent chez NICE Actimize, répond à trois questions de Finyear pour donner à apprécier le cadre et expliquer pourquoi le blanchiment d'argent va se développer : **Tony Wicks**

Pourquoi est-ce que l'action de SWIFT favorise le développement du blanchiment d'argent ?

L'action de SWIFT entraine depuis le samedi 16 mars l'impossibilité pour 25 institutions financières iraniennes d'envoyer et de recevoir des transactions, des titres et des échanges commerciaux au travers de son réseau SWIFT. Chaque année, ce sont près de dix milliards d'échanges qui transitent via SWIFT et une petite fraction d'entre eux, de l'ordre de 0,03%, provient ou est adressée à des banques en Iran. Cette fraction peut sembler minime, mais dans l'environnement actuel des sanctions, elle a une importance significative.

Le blocage du réseau SWIFT est possible parce que la société est basée en Belgique et par conséquent dans l'obligation de suivre le régime de sanctions déterminées par l'Europe. Cela a une incidence non seulement sur les sociétés européennes mais également sur les transactions avec les principaux acheteurs de pétrole brut en Inde, en Corée du Sud, en Afrique du Sud et en Chine. La position européenne a donc des effets extra-territoriaux évidents. Son impact est supérieur en termes d'effets que les récentes sanctions et restrictions européennes sur l'importation de pétrole. Si la Chine veut continuer à en acheter, elle sera confrontée à une grande difficulté pour payer !

Sans canal légal de transferts de fonds, les gestionnaires de fonds iraniens vont devoir se reporter vers un système bancaire alternatif, illégal, dit Shadow banking (dérivé du Hawala Banking) et emprunter de nouvelles méthodes commerciales.

Quels sont les meilleurs moyens pour blanchir de l'argent ?

Dans ce contexte, l'argent va circuler par le biais de méthodes commerciales informelles, via des chaînes complexes d'intermédiaires. Pour mémoire, à la suite des attaques terroristes de 2001, SWIFT a été invité à fournir des informations sur certaines transactions au gouvernement américain dans le cadre du Programme Terrorist Finance Tracking. Ironiquement, le blocage des transactions aujourd'hui va rendre plus difficile la connaissance approfondie de la prolifération des activités et le canal emprunté qui étaient auparavant observables. Les transactions qui vont passer en Shadow Banking disparaîtront purement et simplement des radars.

Si des mouvements d'argent s'évanouissent dans le Shadow Banking ; ils doivent tout de même réapparaître dans le système financier à un moment ou à un autre via des centres d'affaires ou des institutions. Il convient dans ce cas d'être très attentif aux changements de volumes d'activités, en particulier chez les états limitrophes de l'Iran

Les banques et les régulateurs rechercheront les variations inhabituelles dans les nouvelles transactions sur les réseaux financiers. Il est assez vraisemblable en outre que les exportations de pétrole iranien se règlent avec des moyens de paiement physiques et via du blanchiment d'argent basé sur des échanges indirects. Cela sera beaucoup plus difficile à repérer.

Quel sera l'impact sur les banques européennes ?

De nombreuses institutions accueillent avec soulagement la clarté que ce changement implique et seront plus rassurées en sachant que les transactions sur le réseau SWIFT ne pourront plus provenir ou être reçues par des institutions iraniennes. La modification réduit également la probabilité de voir des transactions redirigées, masquées, ou de constater des champs du message de paiement effacés. Dans l'absolu, cela ne change pas l'obligation des institutions d'appliquer des contrôles et des sanctions – d'autant que les entités iraniennes sur les listes n'agissent pas seulement à l'intérieur de l'Iran. Certaines d'entre elles sont à présent contraintes de chercher de nouveaux canaux pour déplacer les fonds à l'intérieur ou à l'extérieur de l'Iran, pour qu'il n'y ait aucun relâchement dans les contrôles et sanctions actuels. Il sera en réalité plus difficile d'identifier les entités sous le coup de sanctions quand elles effectueront des paiements à partir des pays limitrophes. Elles continueront de dissimuler leur véritable identité et emprunteront les voies du Shadow Banking (comme le Hawala banking) plutôt que les canaux financiers traditionnels.

Liens : http://www.finyear.com/Consequence-de-l-interruption-du-reseau-SWIFT-en-Iran-Tony-Wicks-NICE-Actimize_a22590.html

SWIFT | Professionnels de la finance : garder en tête la blockchain

Les directives sur les services de paiement et la lutte anti-blanchiment relèvent les défis de la réglementation des tiers prestataires de services de paiement

Une nouvelle recherche universitaire du SWIFT Institute analyse les dernières réglementations sur les paiements, qui identifie des lacunes et des conséquences, et présente des recommandations afin d'aider à clarifier les nouvelles politiques.

SWIFT Institute annonce la disponibilité d'une nouvelle recherche qui analyse la régulation des tiers prestataires de services de paiement et des monnaies virtuelles.

Intitulé "The evolution of third party payment providers and cryptocurrencies under the European Union's PSD2 and AMLD4", ce document évalue de manière critique la législation en vigueur et les initiatives législatives en cours pour les tiers prestataires de services de paiement. Il met également en évidence le potentiel de réglementation des crypto-monnaies en termes de lutte contre le blanchiment d'argent et le financement du terrorisme.

L'étude met l'accent sur les développements réglementaires au sein de l'UE, notamment les directives PSD2 (Payment Service Directive) sur les services de paiements et AMLD4 (Fourth Anti-Money Laundering Directive) sur la lutte contre le blanchiment d'argent. Elle comprend également un point de vue étendu sur les marchés nord-américains et asiatiques.

« Au cours de la dernière décennie, l'influence des nouvelles technologies et des méthodes de communication a considérablement changé le paysage financier » indique Peter Ware, Directeur du SWIFT Institute. « Partout dans le monde, de nouveaux cadres juridiques ont été adoptés afin de réglementer les acteurs autres que les établissements de crédits. Cependant, ces cadres juridiques manquent encore de clarté concernant deux nouveaux types d'acteurs : les tiers prestataires de services de paiement et les monnaies virtuelles ».

Selon l'étude, les tiers prestataires de services de paiement permettent aux consommateurs de réaliser des paiements en ligne sans avoir besoin de recourir à une carte de crédit, en établissant « un lien entre le payeur et le commerçant en ligne via le module bancaire en ligne du payeur ». Le consommateur n'a pas besoin d'ouvrir un compte directement chez eux. A la place, ces tiers rassemblent des informations sur les comptes existants des consommateurs et présentent ces informations de manière intégrée. Ils fournissent une passerelle à partir de laquelle les clients se connectent à leurs comptes bancaires en utilisant leurs références et identifiants uniques. En agissant de la sorte, ces tiers arrivent à acquérir un nombre important d'informations sensibles.

Les monnaies virtuelles sont majoritairement utilisées dans les systèmes de paiement qui ne reposent pas sur les acteurs traditionnels tels que les banques et les fournisseurs de services de paiement. L'exemple le plus notable est celui des devises cryptées – comme le bitcoin – qui sont décentralisées et ont recours à des pseudonymes pour leurs transactions.

L'étude conclut que même si les directives PSD2, AMLD4 et autres réglementations sont un pas dans la bonne direction, certains aspects restent à éclaircir et nécessitent davantage d'attention. Par conséquent, le rapport propose des recommandations aux organismes de réglementation et aux professionnels de la finance.

Recommandations pour les organismes de réglementation :

1. Eclaircir les ambigüités qui subsistent
2. Harmoniser le cadre législatif de l'Union européenne
3. Coordonner les initiatives réglementaires internationales
4. Eviter une approche locale concernant les monnaies virtuelles
5. Adopter une perspective rationnelle sur les monnaies virtuelles

Recommandations pour les professionnels de la finance :

6. Regarder au-delà des forces disruptives

7. Nécessité de conformité
8. Ne pas systématiquement rejeter les monnaies virtuelles
9. Garder en tête la Blockchain

Les recherches ont été entreprises par Nathan Van De Velde, Niels Van De Zande et Peggy Valcke de l'Université belge KU Leuven et ont récemment été présentées lors de la conférence annuelle SIBOS de SWIFT à Singapour.

NOTES

La Directive relative aux services de paiements (PSD2), adoptée par le Parlement européen en octobre 2015 est une législation de l'Union européenne qui améliore la protection des consommateurs, favorise l'innovation et augmente la sécurité des services de paiement.

Le quatrième Directive anti-blanchiment (AMLD4), qui a finalement été adoptée en mai 2015, fait partie d'un ensemble de mesures visant à empêcher l'utilisation du système financier à des fins de blanchiment de capitaux ou de financement du terrorisme.

A propos du SWIFT Institute

Lancé en avril 2012, le SWIFT Institute encourage la recherche indépendante afin d'étendre la compréhension des pratiques actuelles et des futurs besoins au sein du secteur financier. Dirigé par SWIFT, et travaillant en étroite collaboration avec des professeurs de grandes universités internationales, le SWIFT Institute rassemble l'industrie financière et les universitaires afin de partager des connaissances et d'engager des réflexions sur des importants à l'échelle mondiale.

Les recherches couvrent différents aspects des transactions bancaires et incluent les domaines suivants : paiements, systèmes de compensation et de règlement, cash management, trade finance, trust et titres

www.swiftinstitute.org.

À propos de SWIFT

SWIFT est une société coopérative qui permet aux membres de son réseau d'échanger des informations financières standardisées et automatiques de manière sûre et fiable, et, dès lors, de réduire les coûts, de limiter les risques opérationnels et de supprimer des processus opérationnels inefficaces. Plus de 10 800 organismes bancaires, établissements financiers, institutions et entreprises dans plus de 200 pays bénéficient des produits et services et de l'expertise de SWIFT et de sa plateforme de communication sécurisée unique au monde. SWIFT assure l'échange sécurisé de données propriétaires en garantissant confidentialité et intégrité. SWIFT facilite également le rapprochement des acteurs de la communauté financière pour élaborer ensemble des pratiques de marché, définir des standards et envisager des solutions aux questions d'intérêt commun. En utilisant SWIFT, les clients peuvent bénéficier d'un large panel de solutions métiers et optimiser la gestion des flux financiers.

Liens : http://www.finyear.com/SWIFT--Professionnels-de-la-finance-garder-en-tete-la-blockchain_a34775.html

Swift :
Le réseau banquier international fait face à une grosse attaque de hackers

Selon une lettre que Swift s'apprête à envoyer vendredi à ses utilisateurs, les méthodes de ces hackers présentent des similitudes avec l'attaque qui avait permis en février à des malfaiteurs de dérober 81 millions de dollars sur un compte de la Banque centrale du Bangladesh auprès de la Réserve fédérale à New York.

Le FBI soupçonne que les malfaiteurs de février avaient bénéficié de complicités internes, avait affirmé mardi le Wall Street Journal.

Le même jour, des hauts représentants de la Réserve fédérale de New York, de la Banque du Bangladesh et du système de paiement international Swift, se sont rencontrés à Bâle, en Suisse, pour discuter de cette fraude cybernétique.
L'attaque menée contre Swift -Society for Worldwide Interbank Financial Telecommunication- montre une véritable tentative pour obtenir un accès à ce système indispensable pour le fonctionnement du monde financier international, selon le texte que s'apprête à publier Swift, cité par le New York Times et le Wall Street Journal.
Cette fois-ci, l'attaque visait une banque commerciale dont elle ne donne pas le nom, et dont les malfaiteurs ont réussi à s'approprier les codes pour envoyer des messages au nom de la banque.
En février, des messages semblant provenir de la Banque du Bangladesh avaient ordonné le transfert vers différents comptes aux Philippines de 81 millions de dollars.
Les méthodes utilisées par les hackers dans ces deux cas « montrent clairement une connaissance approfondie et sophistiquée des opérations de ce type dans les banques visées », selon la lettre de Swift, toujours citée par les journaux.
https://www.koldanews.com/2016/05/13/swift-le-reseau-banquier-international-fait-face-a-une-grosse-attaque-de-hackers-a539130.html

Le protocole bancaire SWIFT victime de cyber fraude

Sécurité : 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.
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.

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.

http://www.zdnet.fr/actualites/le-protocole-bancaire-swift-victime-de-cyber-fraude-39836064.htm

Paiements internationaux : Swift prépare sa mue 2.0

La messagerie bancaire sécurisée s'engage à effectuer les transferts d'argent internationaux en un jour d'ici un an. 21 banques expérimentent de nouveaux processus d'échanges entre elles.

Le système de messagerie bancaire sécurisée Swift prend le taureau par les cornes. La coopérative de banques et d'institutions financières, dont l'infrastructure est utilisée par près de 11.000 membres dans quelque 200 pays pour garantir l'échange de données financières réalisé lors d'un paiement ou d'un achat de titres, a décidé de « *réinventer les paiements internationaux sur la base de nouveaux standards* ". Elle a lancé pour ce faire en décembre dernier un plan baptisé « Global payment innovation initiative " auquel se sont ralliées 45 banques fin janvier.

Sur ces 45 établissements qui couvrent 67 % des échanges transfrontaliers traités par Swift, 21 lancent un pilote qui doit d'ici l'automne faire la preuve que le réseau de banques correspondantes de la messagerie, vieux de près de 45 ans, reste pertinent et compétitif face à de nouveaux entrants.

Les chiffres clefs

45 institutions financières se sont engagées à adopter de nouvelles règles d'échanges à partir de 2017.

67% des paiements internationaux traités par Swift devraient alors être réalisés en un jour.

En pratique, les établissements participants s'engagent à ce qu'un transfert d'argent par une grande entreprise cliente, fait au sein du réseau international des banques pilotes, soit crédité en un seul jour ouvré. C'est en effet là que le bât blesse : une opération qui transite via Swift prend aujourd'hui au minimum trois jours et le délai peut aller jusqu'à neuf jours selon la complexité du transfert. Ce, sans que le client ne soit informé sur l'état d'avancement de l'opération ni assuré du délai exact pour que l'argent transféré le soit réellement, ni qu'il soit

sûr du coût précis de l'opération. Ces incertitudes sont devenues incompréhensibles voire intolérables dans un monde où l'instantanéité est devenue la norme. Elles font d'ailleurs le succès de nouveaux acteurs comme Transferwiseou Paypal.

Plan stratégique

« *La messagerie Swift n'est pas du tout en cause, ce sont les pratiques des banques du réseau en matière de transfert qui doivent être réinventées* », souligne Thierry Chilosi, responsable Market initiatives chez Swift. Autrement dit le fonctionnement du réseau de banques correspondantes chargées d'acheminer le transfert doit être sérieusement dépoussiéré et c'est ce à quoi se sont engagés les 21 établissements du pilote via un corpus de nouveaux accords de services multilatéraux proposés par Swift. Cet ensemble de règles devra être validé à la conférence annuelle Sibos organisée par la messagerie internationale à Genève fin septembre, avant d'être étendu aux 45 banques volontaires en 2017.

http://www.lesechos.fr/14/03/2016/lesechos.fr/021765608971_paiements-internationaux---swift-prepare-sa-mue-2-0.htm

Banque de l'Equateur piratée, 12 millions de dollars dérobés via SWIFT

La banque du Bangladesh n'est pas la seule victime des récents "cyber-hold-up". Après la récente attaque ayant visé la banque de l'Equateur (12 millions de dollars dérobés), cela ressemble de plus ne plus à une cyberattaque généralisée visant le système bancaire mondial…

Il s'agit là d'une énième cyberattaque de banque, au cours de laquelle les cybercriminels ont directement cible le système SWIFT, utilisé par l'ensemble de l'écosystème financier mondial. La cible : la banque de l'Equateur. Le bilan : 12 millions de dollars dérobés par les pirates informatiques.

Cela devient une évidence que tout le monde peut remarquer : le système bancaire international basé sur SWIFT est bien attaqué, comme le prouvent les récents cyber-casses ayant visé de nombreuses banques de moindre sécurité. Si l'on ajoute ces récents 12 millions volés à une banque équatorienne (Banco del Austro) aux 81 millions de la banque du Bangladesh, cela montre bien l'aspect critique de la situation.

L'attaque de Banco del Austro en Equateur aurait eu lieu en janvier 2015, information révélée par le biais d'un procès intenté par la banque contre Wells Fargo, une banque basée à San Francisco, comme l'a rapporté Reuters.

Voici comment les cyber-criminels ont ciblé ces banques :

- Utilisation de logiciels malveillants sophistiqués pour contourner les systèmes de sécurité locaux de la banque
- Gagner l'accès au réseau de messagerie SWIFT interne
- Envoi de messages frauduleux via SWIFT pour initier les transferts de fonds à partir de comptes vers de plus grandes banques

Pendant plus de dix jours, les pirates ont pu avoir la main sur le système SWIFT d'un employé de la banque, et ainsi, modifier les détails des transactions d'une douzaines de transferts pour un montant total dépassant les 12 millions de dollars, transféré sur des comptes à Hong Kong, Dubaï, New York et Los Angeles.

Durant le procès devant un tribunal de New York, Banco del Austro tient Wells Fargo responsable de ne pas avoir repéré les transactions frauduleuses et a exigé de la banque de lui rembourser le montant total qui lui a été volé. Selon BDA, tout cela aurait pu être évité si les deux organismes avaient partagé de plus amples informations sur SWIFT.

Wells Fargo a bien entendu également riposté et a directement blâmé les faiblesses des politiques et des procédures de sécurité au sein de Banco del Austro, ayant permis le cyber-braquage. Pour Wells Fargo, les transactions ont été bien traitées par rapport aux instructions fournies, reçues via des messages SWIFT authentifiés et donc non repérés comme frauduleux.
Selon les rapports, la cyberattaque est longtemps restée secrète. D'après les divers communiqués sur l'affaire, le brèche n'est pas identifiée et aucun des partis n'a d'explications précises sur le pourquoi du comment…
"*Nous ne savions pas*", a déclaré SWIFT dans un communiqué. "*Nous avons besoin d'être informés par les clients de ces fraudes si elles se rapportent à nos produits et services afin que nous puissions informer et soutenir la communauté. Nous avons été en contact avec la banque concernée pour obtenir plus d'informations, et nous rappelant les clients de leur obligations de partager ces informations avec nous.*"
Les rapports montrent que la sécurité de SWIFT même n'a pas été violée durant l'attaque, mais que les cybercriminels ont utilisé un logiciel malveillant de pointe pour voler directement les informations d'identification aux employés de la banque et ainsi, couvrir leurs traces.
Le malware en question avait déjà été utilisé lors de l'attaque ayant visé la banque du Bangladesh, et avait permis aux cybercriminels de manipuler à leur guise les journaux d'historique des systèmes et de faire disparaître toute trace des transactions frauduleuses. A suivre.
https://www.undernews.fr/banque-cartes-bancaires/banque-de-lequateur-piratee-12-millions-de-dollars-derobes-via-la-faille-swift.html

Bitdefender : L'un des serveurs de l'éditeur piraté, chantage à la clé

L'éditeur roumain de solution de sécurité Bitdefender a été victime d'un piratage de l'un de ses serveurs.
Le cybercriminel aurait dérobé des données personnelles d'utilisateurs et tente de faire chanter la firme en exigeant de l'argent en échange de son silence.
Il se fait appeler *DetoxRansome* et aurait réussi à s'emparer de données d'identification confidentielles d'utilisateurs présente sur un serveur de la firme. Il est malheureux qu'un piratage puisse toucher une entreprise de sécurité mais ce n'est pas tout… attendez la meilleure !

Des données en clair non chiffrées

Et oui ! Le pirate a pu accéder aux données d'identification d'un échantillon représentant 1% de la clientèle PME.
Afin de prouver ses dires, le pirate a fourni une liste de noms d'utilisateurs et de mots de passe pour plus de 250 comptes clients dont certains ont été confirmés comme étant actifs.
Bitdefender confirme la brèche et ajoute que la base ne contenait que quelques comptes apprenant à des PME, mais que les comptes des grandes entreprises et ceux des particuliers n'ont pas été compromis.
La surprise réside surtout dans le fait que les mots de passe étaient tous en clair et non chiffrés/hashés.
Très étonnant (voir décevant) de la part d'une telle firme de sécurité informatique. Espérons que cela va être amélioré prochainement.
Sur le Web underground, le pirate DetoxRansome a mis en vente les données pour 8
Bitcoins et précise que la vulnérabilité provient du service Amazon Elastic Web qui a souvent des problèmes avec le SSL. L'erreur est humaine, et c'est via une technique

de sniffing que ce dernier a pu compromettre les données privées, comme l'explique Hack Film. Bref, aucune vulnérabilité zero-day n'est en cause.
« Au cours d'une montée de version de l'infrastructure, un seul serveur a été déployé avec un package logiciel plus à jour contenant une faille connue, ce qui a permis d'extraire des informations dessus mais pas de compromettre le système dans son ensemble », a précisé Catalin Cosoi, responsable de la sécurité chez Bitdefender.
Tous les mots de passe touchés ont été réinitialisés depuis et une enquête approfondissement est en cours.

Du chantage et une rançon à la clé

Le pirate demande une rançon de 15 000 dollars en échange de la non divulgation des données.
"La question a été immédiatement résolu, et des mesures de sécurité supplémentaires ont été mis en place pour empêcher qu'elle ne se reproduise," a déclaré le porte- parole de la société dans un communiqué. "Notre enquête a révélé qu'aucun autre serveur ou services ont été touchés."

Lien : https://www.undernews.fr/hacking-hacktivisme/bitdefender-lun-des-serveur-de-lediteur-pirate-chantage-a-la-cle.html

BitDefender révèle une tendance inquiétante pour la sécurité des cartes bancaires

Une récente étude de BitDefender révèle une tendance inquiétante pour la sécurité des cartes bancaires : plus d'une personne sur deux déclare révéler des données confidentielles en répondant sur internet à des requêtes potentiellement frauduleuses.
BitDefender, éditeur de solutions de sécurité pour Internet publie aujourd'hui les résultats d'une nouvelle étude révélant des statistiques inquiétantes quant à la protection des données de cartes bancaires.
97% des 2 210 personnes interrogées, âgées de 18 à 65 ans, ont déclaré avoir acheté des biens et des services en ligne. Parmi celles-ci, 57% ont reconnu fournir à la demande des données bancaires personnelles et confidentielles, risquant ainsi d'être victimes de fraude ou de voir leurs comptes bancaires piratés.
L'étude a également révélé que 27% des personnes composant le panel ignoraient le l'existence possible de faux sites Web et des escroqueries de type « phishing ». Le phishing consiste à se faire passer pour une organisation ou un tiers de confiance dans le but d'obtenir des informations confidentielles telles que des noms d'utilisateurs, des mots de passe et des informations relatives aux cartes bancaires, au travers de communications électroniques.
« Malheureusement, il est avéré qu'une simple recherche en ligne permet à tout le monde de trouver facilement des identifiants de cartes bancaires exploitables. Un grand nombre de cybercriminels se sont organisés pour en faire une activité lucrative et vendent ce type d'informations pour toute sorte de montant.» rappelle Stéphane Pacalet, Directeur Général d'Editions Profil en charge de la commercialisation des solutions BitDefender en France.
https://www.undernews.fr/banque-cartes-bancaires/bitdefender-revele-une-tendance-inquietante-pour-la-securite-des-cartes-bancaires.html