DEVLHON
CONSULTING

TOP 10 des Cyberattaques Bancaires en 2018

Selon Kapersky Lab, entreprise dédiée à la sécurité informatique dans plus de 200 pays, les cyberattaques continuent à augmenter et 2019 ne sera pas l'exception.

« Début 2018, le président du Forum Economique Mondial a annoncé que les pertes mondiales résultant des cyberattaques atteignaient près de 1000 milliards USD»

Les Chiffres

Faits marquants

Le nombre de cyberattaques a augmenté régulièrement au cours des dernières années. Selon Kaspersky Lab, 1876 millions d'attaques malveillantes ont eu lieu en 2018 et tout indique que 2019 ne sera pas l'exception pour que ce chiffre continue à augmenter. Le secteur bancaire est, par sa nature, une cible de plus en plus attirante pour les acteurs malveillants.

Début 2018, le président du Forum Economique Mondial a annoncé que les pertes mondiales résultant des cyberattaques atteignaient près de 1000 milliards USD . Aujourd'hui, les banques subissent actuellement des attaques ciblant les virements interbancaires, le traitement des cartes, les distributeurs d'argent, la banque en ligne et les passerelles de paiement. L'éventail des cibles est vaste. Si les hackers disposent des connaissances et des moyens techniques nécessaires, l'accès à de tels systèmes peut générer plus de revenus que la fraude à l'encontre des clients des banques. Pour voler de l'argent, les criminels doivent pénétrer dans l'infrastructure de la banque, qui est généralement complexe. Néanmoins, les criminels parviennent toujours à contourner tous les mécanismes de protection et les médias continuent de faire état de nouvelles cyberattaques et vols de banques.

Les Etapes d'une cyberattaque

Les intrus choisissent leur cible en grande partie en fonction de leur expertise technique, des outils disponibles et des connaissances des processus bancaires internes. Chaque attaque est légèrement unique: par exemple, les attaquants peuvent agir différemment au stade du retrait d'argent. Cependant, il y a aussi des caractéristiques communes que nous aborderons dans cette section. Les attaquants opèrent selon des scénarii assez simples comprenant les cinq étapes principales indiquées dans la figure ci-dessous.

Figure 1 - Etapes d'une cyberattaque. Source : Positive Technologies

« … Les pirates informatiques, identifiés par FireEye comme étant APT38, ont infiltré plus de 16 organisations dans 11 pays, dont les États-Unis, et volé plus de 100 millions de dollars »

Top 10 des Cyberattaques Bancaires 2018

Voici un extrait des cyberattaques les plus importantes dans le secteur bancaire en 2018

1. **Plusieurs Banques. 2014-2018, Monde. Montant : 100 Millions USD**

Un groupe de pirates informatique nord-coréen a tenté de voler au moins 1,1 milliard de dollars après une série d'attaques contre des banques mondiales au cours des quatre dernières années (2014-2018), selon la société de cybersécurité FireEye Inc. Les pirates informatiques ont infiltré plus de 16 organisations dans 11 pays, dont les États-Unis, et volé plus de 100 millions de dollars. En janvier 2018, la banque mexicaine appartenant à l'État a déjoué la tentative de vol de 110 millions de dollars à l'aide de méthodes similaires. En mai, une banque chilienne a perdu 10 millions de dollars. Les deux attaques ont été menées par APT38 (nom du groupe pirate), a déclaré FireEye dans le rapport.

2. **Banques de l'Europe de l'Est. Montant : +30 Millions USD**

En 2018, les spécialistes de Kaspersky Lab ont été invités à enquêter sur une série d'incidents. Chaque attaque avait un tremplin commun : un périphérique inconnu directement connecté au réseau local de la société. Au moins huit banques d'Europe de l'Est ont été la cible de ces attaques (appelées collectivement DarkVishnya), qui ont causé des dommages évalués à plusieurs dizaines de millions de dollars.

3. **Cosmos Bank. 2018, Inde. Montant : 13.5 Millions USD**

Une cyberattaque contre une banque indienne a créé de pertes de 944 millions de roupies, soit 13,5 millions USD. Selon Reuters, l'attaque s'est produite le 11 août 2018 à travers plusieurs retraits simultanés dans les distributeurs de 28 pays de la banque indienne Cosmos Bank. L'attaque consiste en un malware injecté sur le serveur de guichet automatique (ATM), ce qui a généré près de 15 000 transactions en un peu plus de 2 heures. Les pirates ont également transféré 139 millions de roupies sur le compte d'une société basée à Hong Kong. Pour ce faire, ils ont utilisé le réseau mondial de paiements SWIFT. Les informations sur la transaction proviennent d'une plainte de la police vue par le média.

4. **BankIslami. Octobre 2018. Montant : 6 Millions USD**

BankIslami, une banque pakistanaise basée à Karachi, a signalé une cyberattaque sur son système de cartes de paiement en Octobre 2018. Selon la déclaration faite par la banque à

la Bourse du Pakistan le 27 octobre 2018 au matin, ils ont détecté une activité suspecte sur l'un de ses systèmes de cartes de paiement internationales et des pirates informatiques ont volé un montant de 2,66 millions de roupies. Dès sa détection, la banque a immédiatement pris des mesures de précaution et a fermé le mécanisme de paiement international. Selon les rapports de fournisseurs de paiement internationaux, le montant perdu serait d'environ 6 millions de dollars.

5. **City Union Bank Ltd. Février 2018, Inde. Montant : 2 Millions USD**

La banque City Union Bank (CTBK.NS) indienne a déclaré en février 2018 que des cybercriminels avaient piraté ses systèmes et transféré près de 2 millions de dollars via trois envois de fonds non autorisés à des prêteurs à l'étranger via la plate-forme financière SWIFT.

6. **Caisse d'Epargne. Avril 2018, France & Russie. Montant : 800.000 USD / 21.000€**

Le jackpotting consiste à vider les distributeurs automatiques à l'aide d'une simple clé USB et d'un ordinateur. Un hacker a été pris en fragrant délit de piratage d'un distributeur automatique de billets de la Caisse d'Épargne. Il avait réussi à voler plus de 21 000 euros. Cependant, l'attaque a été bien réussie en 2017, quand 8 machines de 2 banques russes ont ainsi été vidées de leur contenu en une seule nuit, pour un butin estimé à 800 000 USD.

7. **Banques Pakistanais. Perte des données : +19.000 Cartes Bancaires**

Des données provenant de 19 864 cartes appartenant à des clients de 22 banques pakistanaises ont été mises en vente sur le Dark Web (un réseau sur internet souvent illégal), selon une analyse réalisée par l'équipe pakistanaise Computer Emergency Response Team, PakCERT. Tout a commencé mi-octobre 2018 lorsque certains clients de la banque BankIslami ont reçu des SMS les alertant des transactions (retrait d'argent), qu'ils n'avaient pas fait. Constatant des transactions anormales de 2,6 millions de roupies, la banque Islami a bloqué son système de paiement international. A ce jour, des analyses sont toujours en cours, mais cela reste l'attaque la plus importante qui a eu lieu jusqu'à présent au Pakistan.

8. **Bank of Montréal & Imperial Bank of Commerce. Perte des données 90k Clients.**

La Banque de Montréal et Canadian Imperial Bank of Commerce ont déclaré en Mai 2018 que des cyber-attaquants pourraient avoir volé les données de près de 90 000 clients lors de ce qui semblait être la première attaque importante contre des institutions financières au Canada. Les 2 banques ont déclaré contacter les clients et leurs conseillers afin de surveiller leurs comptes

et de signaler toute activité suspecte. Même si l'attaque n'a pas été confirmée, les actions des 2 banques ont perdu environ 0,3%.

9. US et Russie. Q2-2018. Chevaux de Troie de Banques Mobiles.

Les chevaux de Troie des services bancaires mobiles sont attrayants pour les cybercriminels qui recherchent un bénéfice facile, selon Kaspersky. Le logiciel malveillant est généralement déguisé en une application légitime pour inciter les gens à l'installer. Une fois l'application bancaire lancée, le cheval de Troie affiche sa propre interface superposant l'interface de l'application. Lorsque l'utilisateur entre des informations d'identification, le logiciel malveillant vole les informations.

Toutefois, tous les pays ne sont pas également menacés. Les hackers ciblent davantage les banques américaines, russes et polonaises. A l'inverse, les établissements français restent à l'abri des logiciels malveillants : seulement 0,1% des attaques détectées au deuxième trimestre ont visé la France. L'une des explications s'inscrit dans la législation particulièrement protectrice pour les victimes. Le code monétaire et financier obligeant les banques à rembourser les sommes dérobées, celles-ci sont de fait incité à concevoir des applications robustes.

10. UK Banks. Attaque DDoS. Montant : Moins de 1 Million £

Sept des plus grandes banques du Royaume-Uni, dont Santander, Royal Bank of Scotland et Tesco Bank, ont été contraintes de réduire leurs activités ou de réinitier des systèmes entiers à la suite d'une cyber-attaque en 2018 à l'aide d'un logiciel pouvant être loué pour seulement 11£, selon le National Crime Agence. Des informations détaillées sur les attaques, qui selon la NCA auraient coûté des centaines de milliers de livres aux banques, ont été révélées à la suite d'une enquête policière internationale visant à fermer Webstresser, un site Web utilisé par les cybercriminels pour lancer de prétendues attaques par déni de service (DDOS) afin d'inonder et désactiver les systèmes informatiques générant un trafic Internet important.