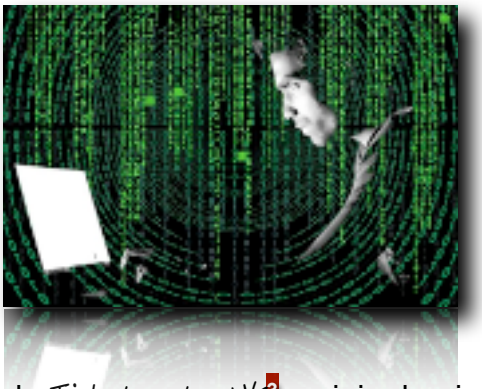
13/09/2018
Gilbert KALLENBORN
Journaliste

Magecart, le groupe de pirates qui sème la terreur sur les sites de commerce en ligne

Ticketmaster, British Airways, Feedify... Des pirates spécialisés sur le vol de données de cartes bancaires montrent que les systèmes e-commerce ne sont pas assez sécurisés.



La semaine dernière, British Airways a révélé être la victime d'un redoutable piratage, impliquant le vol de 380.000 données de cartes bancaires[1] (numéros, date de validité et code de sécurité à trois chiffres - CVV). Le communiqué de la compagnie ne donne que peu de détails techniques sur cette affaire. Mais après avoir analysé des données web, le chercheur en sécurité Yonathan Klijnsman[2] de RiskIQ est arrivé à la conclusion que cette opération est l'œuvre du groupe de pirates Magecart. Celui-ci sévit sur la Toile depuis plusieurs années et a notamment été à l'origine du piratage de Ticketmaster UK[3] en juin dernier.

Dans les deux cas, un grand nombre de données de cartes bancaires ont été dérobées. Toutefois, la technique de piratage est sensiblement différente. Dans l'affaire Ticketmaster, les pirates avaient réussi à hacker les serveurs d'un sous-traitant qui fournissait au spécialiste de la billetterie en ligne un service de support implémenté sous la forme d'un Javascript. En insérant leur malware dans ce code, les pirates ont réussi à mettre la main sur les données de cartes bancaires que les clients renseignaient sur le site de Ticketmaster.

Une attaque ciblée

Dans le cas de British Airways, les pirates ont, semble-t-il, hacké directement les serveurs de British Airways et réussi à injecter leur code malveillant dans la librairie Javascript Modernizr, comme a pu le vérifier Yonathan Klijnsman.

Ce code malveillant permettait aux pirates de détecter le remplissage d'un formulaire de paiement sur le site web de British Airways. Au moment où le client validait ce formulaire, une copie des données de cartes bancaires était alors envoyée automatiquement vers un serveur tiers hébergé sur le domaine baways.com, controlé par les pirates. Contrairement au hack de Ticketmaster, cette attaque

[1] https://www.01net.com/actualites/british-airways-des-pirates-ont-vole-les-donnees-de-cartes-bancaires-de-ses-clients-1519156.html

[2] https://www.riskiq.com/blog/labs/magecart-british-airways-breach/

[3] https://www.01net.com/actualites/un-grand-nombre-de-numeros-de-cartes-bancaires-derobes-chez-ticketmaster-1480695.html

était donc beaucoup plus ciblée, avec un code créé sur mesure pour le formulaire de la compagnie aérienne.

RiskIQ - En rouge, le code malveillant ajouté par les pirates

Et nous n'en sommes qu'au début. Car visiblement, les pirates de *Magecart* ne se donnent aucun répit. Hier, le chercheur en sécurité *Placebo* a découvert leur présence dans les scripts de *Feedify*, un service de support en ligne utilisé par plus de 4000 sites web. Pour les internautes, le risque est donc maximal.

> Magecart on Feedify. A customer engagement tool. According to there website 4000+ website use there tooling/code. Fixed today after I notified them. @ydklijnsma @GossiTheDog pic.twitter.com/K2czXkUoHD
> — Placebo (@Placebo52510486) September 11, 2018
> Real data on this first time, compromised for 3 weeks: https://t.co/4DtpP3IOWd
>
> Second time it was this morning: https://t.co/Ohazj6iv72
> — Yonathan Klijnsma (@ydklijnsma) September 12, 2018

Cette série d'attaques pose un grand problème car il risque de détruire la confiance que les internautes peuvent avoir vis-à-vis des achats en ligne. *La nature de ces attaques prouve que les boutiques en ligne ne sont pas assez sécurisées et que la multiplication des sous-traitants augmente le risque de vol de manière exponentielle*. Afin de pouvoir gonfler rapidement leur richesse fonctionnelle, certains sites web n'hésitent pas à intégrer des dizaines de codes tiers. Surveiller l'intégrité de tous ces codes différents et détecter les modifications malveillantes devient alors une véritable gageure.

La e-carte bleue permet de parer ces attaques

En tant que consommateur, comment peut-on se protéger ? Le premier réflexe à avoir est d'activer le service 3D Secure, si votre banque le propose. Il ajoute un second facteur d'authentification sous la forme d'un code à usage unique envoyé par SMS. Dans ce cas, les données de carte bancaire ne sont plus suffisantes pour réaliser des paiements frauduleux. Le problème, c'est que le système 3D Secure n'est pas implémenté par tous les vendeurs en ligne. Le risque du paiement frauduleux n'est donc pas complètement écarté.

Une autre solution est de souscrire à un service de carte bancaire virtuelle ou "e-carte bleue"[4] (lire ci-dessous). Dans ce cas, la banque fournit au client un logiciel qui génère pour chaque achat en ligne un numéro de carte, une date d'expiration et un code CVV. Cette carte à usage unique est en outre plafonnée par le demandeur.

Ces données sont à usage unique et ne peuvent donc pas être réutilisées pour un autre achat. Même si elles sont volées, ce n'est pas grave. En revanche, cette procédure augmente quand même la complexité de l'achat en ligne.

e-Carte Bleue : un surcoût injustifié pour les internautes

09/04/2002
Karine Solovieff

Le GIE Carte Bleue lance le numéro de carte bancaire jetable, valable pour une seule transaction. Sous prétexte d'une meilleure sécurité, l'utilisation de l'e-carte bleue sera payante pour l'internaute.

Après deux ans de développement[5], l'e-Carte Bleue est enfin commercialisée par les banques françaises au travers du GIE Carte Bleue (Groupement d'intérêt économique Carte Bleue).

Son principe est simple[6] : un logiciel installé sur le poste de l'internaute lui génère un numéro de carte bancaire, valable pour une transaction unique. Bien que l'e-Carte Bleue ne soit qu'un prolongement de la Carte Bleue Visa, déjà payante, les banques françaises ont choisi de se rémunérer sur son utilisation par les internautes.

---

[4] https://www.01net.com/actualites/e-carte-bleue-un-surcout-injustifie-pour-les-internautes-181400.html

[5] https://www.01net.com/editorial/137127/mise-a-jour-carte-bleue-une-solution-de-paiement-securise-pour-la-mi-2001/

[6] https://www.01net.com/editorial/170758/ocard-le-numero-de-carte-bancaire-jetable/

Tarif à la carte selon les banques

Chaque banque est libre de fixer ses tarifs. La Société Générale, première banque à ouvrir le bal, prélèvera 50 centimes d'euro par transaction, et six euros à l'inscription. La Caisse d'Epargne Ile de France, qui commencera la vente dans quelques semaines, a opté pour un forfait d'un euro par mois. Le service est ouvert aux porteurs de Carte Bleue Visa, soit 60 % des porteurs de cartes bancaires en France. Il nécessite une inscription auprès de sa banque, qui fournit un identifiant et un mot de passe, indispensables à l'utilisation de l'e-carte bleue.

Pour le commerçant, le processus est invisible. Il ne voit pas la différence entre un numéro de carte normale et un numéro d'e-Carte Bleue. Cela permet à l'e-Carte Bleue d'être utilisée sur n'importe quel site marchand, immédiatement.

Pour le cyber-acheteur, c'est l'assurance que son numéro ne pourra être réutilisé pour un autre achat, par un fraudeur ayant piraté les bases de données du commerçant.

Les banques veulent inquiéter pour mieux rassurer

Le GIE Carte Bleue Visa compte sur l'e-Carte Bleue[7] pour convertir les porteurs de carte en cyber-acheteur. Mais le nouveau service multiplie les contradictions. Tout d'abord, en cherchant à "instaurer la confiance", les banques laissent entendre encore une fois, qu'il existe un risque sur Internet. Une démarche déjà employée par American Express[8] pour le lancement de leur dernière carte bancaire. Pourtant, lors de la conférence de presse de lancement, leurs représentants ont insisté sur le fait qu'il n'existait pas de fraudes sur Internet. Aujourd'hui, les problèmes viennent principalement des numéros récupérés par des escrocs sur les facturettes, ou ceux créés avec des générateurs automatiques. Des problèmes que l'e-carte bleue ne résout pas.

Ensuite, il faut s'inscrire au préalable au service et installer un logiciel, une démarche qui pourrait rebuter les internautes débutants, marché cible de l'e-Carte Bleue. Enfin, même si le GIE estime que "la confiance se mérite et, en l'occurrence, ici elle se paye", comme l'a résumé l'un de ses membres, quel internaute sera prêt à ajouter un coût supplémentaire à ses achats en ligne, alors qu'aujourd'hui la législation française le protège contre les risques de fraude ?

Karine Solovieff

❒ ajout (15-9-2018) : l'utilisation d'une e-carte est maintenant également conditionnée par l'utilisation du système "3D-secure" qui impose que chaque utilisation soit au préalable validée par l'envoi d'un code par sms sur un téléphone inscrit.

❒ l'article date de 2002, époque où la cyber-criminalité était sans doute encore considérée comme marginale. L'évolution dans ce domaine rend la 'e-carte' indispensable à tout achat en ligne.

[7] http://www.e-cartebleue.com/

[8] https://www.01net.com/editorial/141660/amex-surfe-sur-la-peur-dinternet-pour-promouvoir-sa-nouvelle-carte/