Six secondes suffisent pour pirater une carte bancaire

Six secondes suffisent pour pirater une carte bancaire

En multipliant les tentatives sur différents sites, des chercheurs sont parvenus à contourner facilement les systèmes de paiement sécurisés mis en place et ce sans même posséder la carte bancaire physique utilisée.

Votre carte bleue n'est en sécurité nulle part. Sans connaître aucun détail de celle-ci, des pirates peuvent facilement pirater un compte en banque. Il leur suffit simplement d'un ordinateur, d'un accès à Internet et de six secondes, révèlent les chercheurs de l'université de Newcastle, au Royaume-Uni, dans une étude publiée dans le journal académique *IEEE Security & Privacy*(IEEE signifiant Institute of Electrical and Electronics Engineer).
Dans la pratique, les chercheurs ont utilisé une attaque par force brute pour contourner les mesures de sécurité visant à protéger le système de paiement en ligne des fraude. Connectée sur différents sites, l'équipe de chercheurs a généré de façon répétée et continue des variations des différentes informations sécurisés de cartes de paiement (numéro de carte, date d'expiration et cryptogramme visuel) jusqu'à obtenir un résultat favorable. D'après l'étude, c'est vraisemblablement une attaque du genre qui était au cœur de l'attaque informatique contre la filiale bancaire du géant britannique de la distribution Tesco, dont 20.000 clients ont été victimes.

Deux petites faiblesses qui en font une grosse

Si l'attaque parvient à réussir, c'est parce que le système ne détecte en effet pas les échecs répétés sur une même carte si cela se produit sur différents sites, d'autre part, tous les sites ne demandent pas les mêmes informations au même moment, ce qui permet de deviner un champ à la fois.

« Ce type d'attaque exploite deux faiblesses qui ne sont pas trop graves d'elles-même mais lorsque utilisées simultanément présentent un sérieux risque pour l'ensemble du système de paiement », explique dans le communiqué Mohammed Ali, étudiant en doctorat à l'école d'informatique de l'université de Newcastle et auteur principal de l'étude.

Simplement en partant des six premiers numéros de la carte de paiement, qui servent à indiquer la banque et le type de carte et sont donc identiques pour chaque fournisseur unique, *« un pirate peut obtenir les trois informations essentielles pour réaliser un achat en ligne en tout juste six secondes »*. Le délai peut être extrêmement réduit dans les cas où le pirate dispose des numéros de cartes, ce qui risque d'arriver de plus en plus souvent au vue de la récente vague d'intrusions informatiques survenues dans les plus grandes entreprises. Il leur suffit dans ce cas de deviner la date d'expiration – moins de 60 essais puisque la plupart des cartes de crédit sont valides cinq an au maximum -, puis le cryptogramme visuel composé de trois chiffres – ce qui prend dans le pire des cas 1.000 essais.
Mohammed Ali souligne toutefois que cette technique d'attaque par force brute ne marche qu'avec le réseau VISA, *« le réseau centralisé de MasterCard a été capable de détecter l'attaque après moins de 10 essais – même lorsque les paiements étaient répartis sur différentes réseaux »*. Autre point faible de la technique : la confirmation par SMS, que demandent bon nombre de sites d'e-commerce en France…[lire la suite]

Rapport 2015 de l'Observatoire de la sécurité des cartes de paiement
Original de l'article mis en page : Il suffit de six secondes pour pirater une carte bancaire

---

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions de formation, de sensibilisation ou d'audits dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Réagissez à cet article