La banque en ligne N26 : 8 mn pour s'inscrire, 5 mn pour la pirater

Les sessions du 33c3, c'est-à-dire le Chaos Communication Congress se déroulant à Hambourg, réservent toujours des surprises. Dans un atelier intitulé « *Tais-toi et prend l'argent* », l'expert en sécurité Vincent Haupert s'en est pris à la banque en ligne N26 (Number 26) originaire d'Allemagne mais qui a posé ses bagages en France début décembre. Cette banque en ligne promet sur son site Internet une inscription éclair en 8 minutes. Las, en passant par son application mobile, le chercheur a mis 5 minutes pour pirater un compte N26.

A première vue pourtant, les règles de sécurité sont respectées. Sur l'application mobile, pour accéder aux comptes bancaires, il faut s'authentifier via une adresse mail et un mot de passe. En complément un code PIN à 4 chiffres est envoyé pour réaliser une double authentification. De même, lors de son inscription, le client aura renseigné son numéro de téléphone pour que son terminal soit reconnu. Cette association est réalisée via l'envoi d'un token par SMS. Les serveurs de la banque en ligne seront par la suite capables de reconnaître ce smartphone.

Une attaque de l'homme du milieu et une API faiblarde

Et c'est là déjà que le bât blesse. Vincent Haupert a démontré que l'application mobile de N26 sur iOS comme sur Android est vulnérable à une attaque dite de l'homme du milieu (MITM). Concrètement, l'application chiffre les données via HTTPS mais ne vérifie pas les certificats des serveurs de N26. Il suffit donc pour un pirate d'utiliser des faux certificats pour récupérer le trafic entre l'application et les serveurs N26. Une fois placé comme intermédiaire, l'expert a pu prendre le contrôle de l'API N26 et modifier des ordres de virement en temps réel, via le réseau WiFi de l'utilisateur.

Pour récupérer les identifiants du client, Vincent Haupert s'est servi du spear phishing. Là encore carton rouge pour la banque en ligne, elle permet le téléchargement des contacts (mails et numéros de téléphone) dans son application, mais ces données sont en clair dans le système de back-end. Le chercheur s'est donc servi de la base de données dérobée à Dropbox (soit 68 millions de comptes) pour tester son attaque. In fine, il a recensé 33 000 clients de N26. Il aurait donc pu envoyer un mail ciblé avec un lien malveillant leur demandant de changer de mot de passe. En glanant ces informations, on peut appairer alors un autre terminal.

N26 découvre les vertus du Bug Bounty

Une fois ces identifiants récupérés, Vincent Haupert est capable de passer des ordres de paiement directement depuis l'assistant vocal d'Apple Siri. Pour les besoins de son expérience, il a réalisé 1000 petits transferts (1 cents) en 30 minutes sans être détecté par les algorithmes anti-fraude de N26. Enfin pour conclure dans cette avalanche de faiblesses, les échanges via l'API contenaient

également des références de cartes bancaires Mastercard avec une authentification de code à 4 chiffres pour les transferts d'argent. Une attaque par force brute résout ce problème rapidement, surtout que le nombre d'essais est illimité.

Contactée par Vincent Haupert, la « néo-banque » a réagi rapidement en bouchant les trous de sécurité mis en évidence par l'expert. Mieux, elle vient de lancer son programme de recherche de bug. Ce bug bounty portera sur les applications Android et iOS, mais aussi sur les sites .n26.com, .number26.de et .tech26.de. En parallèle, l'établissement bancaire s'engage à subventionner à hauteur de 5000 euros deux théses sur la sécurité informatique.

A lire aussi :

Les cartes Visa piratables en quelques secondes

Sécurité : quand une application mobile peut faire sauter la banque