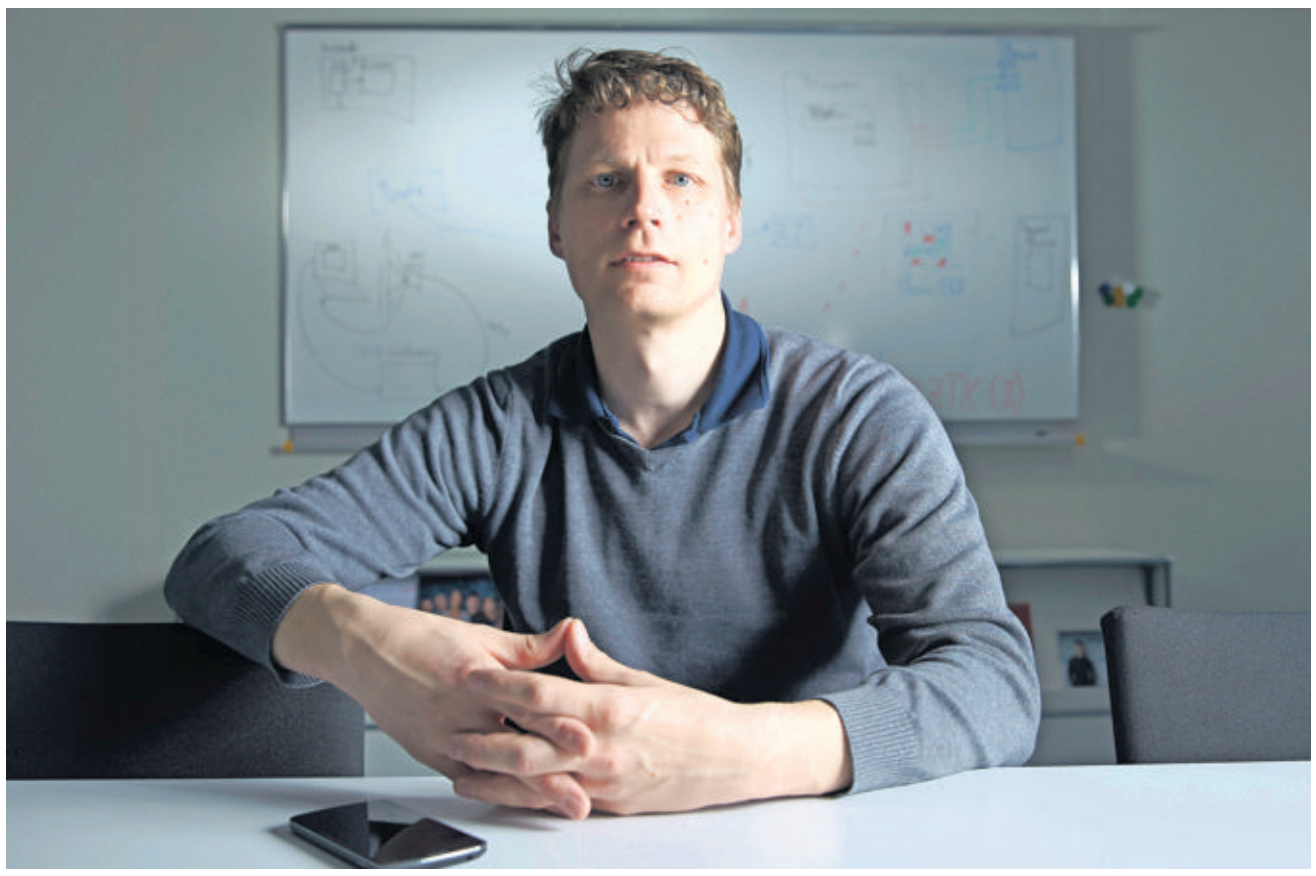
Un chercheur met à mal la sécurité du e-banking depuis un smartphone

PIRATAGE Les versements effectués depuis un smartphone peuvent être facilement manipulés, prévient un professeur à la HES bernoise. Cette vulnérabilité découle du fait que les appareils mobiles ne sont pas sécurisés.

Alexandre Haederli
alexandre.haederli@lematindimanche.ch



Spécialiste de la sécurité de l'information, Reto Koenig recommande d'éviter d'utiliser son smartphone pour faire ses paiements.
Yvain Genevay

Consulter le solde de son compte sur son smartphone? Faire ses paiements depuis son écran tactile? Comme un nombre croissant de personnes en Suisse, Reto Koenig a essayé. «C'est extrêmement pratique, mais j'ai arrêté», tranche ce professeur d'informatique à la HES bernoise.

Il y a quelques mois, Reto Koenig a suggéré à deux étudiants en bachelor de manipuler des transactions passées depuis un appareil mobile. Le binôme a choisi de s'attaquer à un système réputé offrir le maximum de sécurité, portant le nom barbare de «mTAN» et adopté par plusieurs banques en Suisse. «Le principe est simple: pour chaque versement, le client reçoit un SMS contenant un code qu'il doit recopier dans sa plateforme de e-banking, sans quoi le paiement n'est pas validé», explique Reto Koenig. Le SMS rappelle également le montant et le bénéficiaire de la transaction. «Cette solution était tout à fait valable il y a cinq ans, lorsque la majorité des téléphones mobiles savaient uniquement passer des appels et recevoir des messages.» La démocratisation des smartphones change la donne.

Avant, on utilisait un ordinateur pour faire du e-banking et on recevait le SMS de confirmation sur un téléphone. Deux canaux distincts qui compliquaient la tâche aux escrocs: une personne malintentionnée devait avoir accès à l'ordinateur de la victime ainsi qu'à son téléphone. Désormais, cette barrière est tombée: on fait ses paiements et on reçoit le SMS de confirmation sur le même appareil.

Même pas besoin d'un virus

Une pratique d'autant plus risquée que les smartphones constituent, d'un point de vue technique, un environnement très peu sécurisé. Des virus, semblables à ceux qui existent sur les ordinateurs, y ont fait leur apparition. «Nous aurions pu développer un virus qui vole le nom de l'utilisateur et son mot de passe, mais nous avons préféré opter pour une autre tactique, indétectable par les antivirus», poursuit le professeur. Ses étudiants ont simplement profité du fait que les smartphones permettent aux différentes applications de communiquer entre elles. «Le plus inquiétant, c'est qu'il ne s'agit pas d'une faille que l'on peut corriger, mais d'un principe de base nécessaire au fonctionnement des appareils, Android comme iPhone.» L'attaque aura nécessité la création de deux applications basiques: un gestionnaire de SMS et un navigateur Internet. «A première vue, elles n'ont rien de particulier: elles ne contiennent pas de code malicieux et ne requièrent aucune autorisation saugrenue au moment de l'installation, insiste ce spécialiste de la sécurité de l'information. Pour inciter l'utilisateur à les télécharger, on peut imaginer une campagne de publicité expliquant qu'elles sont plus conviviales ou plus sûres que les applications par défaut.»

> «Cette fraude est facile à mettre en place et même un utilisateur averti ne peut la détecter»
> **RETO KOENIG**
> Professeur d'informatique à la HES bernoise

Voici ensuite comment fonctionne le piège mis sur pied à la HES bernoise: vous effectuez depuis votre smartphone un versement de 100 francs vers le compte de Monsieur Dupont. Au moment d'envoyer le paiement, le navigateur frauduleux modifie, sans que l'utilisateur ne puisse s'en rendre compte, le destinataire et le montant de la transaction. Vous recevez ensuite un SMS avec le code de confirmation. A priori, rien à signaler: le message vous demande de confirmer un versement de 100 francs à M. Dupont. Sauf qu'en réalité, l'affichage du bénéficiaire a été trafiqué par l'application SMS. Cette dernière affiche les informations qui lui ont été discrètement transmises par le navigateur. Mais en recopiant le code dans le navigateur, vous allez confirmer la transaction vers le compte choisi par le pirate.

Peu de compétences requises

Le scénario a été testé dans des conditions réelles. «Pas avec une vraie banque, précise Reto Koenig. Les étudiants ont créé le site Web d'une banque fictive.» Et le résultat est bluffant. «J'ai joué le rôle du client et je n'y ai vu que du feu, raconte le professeur. Même un utilisateur averti ne peut pas détecter la fraude.» L'autre point qui inquiète particulièrement le chercheur, c'est la facilité avec laquelle ses étudiants sont parvenus à leurs fins. «Ils avaient des compétences assez standard et n'avaient jamais programmé d'applications pour smartphone, détaille le professeur. Pour l'ensemble du projet, le binôme a travaillé un peu plus de 300 heures seulement. Pour une personne avec un peu d'expérience, cela peut aller beaucoup plus vite.»

Cette démonstration devrait-elle dissuader le client d'utiliser son smartphone pour le e-banking? Pour Reto Koenig, cela ne fait pas un pli. Faut-il privilégier les applications pour smartphone développées par certaines banques? «Même si elles donnent un sentiment de sécurité, le fait qu'elles se trouvent aussi sur un smartphone qui est par définition vulnérable doit inciter à la plus grande prudence.» Paranoïa ou inquiétude légitime? Les banques ne communiquent aucune statistique sur les fraudes liées au e-banking, difficile donc de se faire une idée de l'ampleur du problème. Pour cet expert, la méthode la plus sûre de pratiquer du e-banking est d'utiliser un jeton d'authentification, un «token», mais très peu de banques proposent cette solution. ●

«Les Suisses sont de grands fans de TuneIn»

MOBILE Sur smartphone ou sur tablette, TuneIn donne accès à des milliers de radios du monde entier. En Suisse, cette application est utilisée par plus de 400 000 personnes.

«Nous sommes en quelque sorte le Google de la radio», image Julien Venetz, directeur de TuneIn pour l'Europe, le Moyen-Orient et l'Afrique. Cette application gratuite permet aux auditeurs d'accéder en quelques clics à plus de 70 000 stations, des plus proches, comme la Radio suisse romande, aux plus exotiques, telles que Sonar FM, une chaîne dédiée au rock basée à Santiago au Chili.

La plupart des radios possèdent leur propre application, mais pour ceux qui aiment zapper d'une station à l'autre, TuneIn propose une centralisation bienvenue. Le service est disponible sous forme d'application pour iPhone, iPad et téléphones Android, sur n'importe quel ordinateur via le navigateur Internet ainsi que sur certains appareils de type Logitech Squeezebox.

Interface enrichie

La start-up fondée en 2002 en Californie revendique aujourd'hui 40 millions d'auditeurs, soit davantage que le très populaire service de streaming musical Spotify. «La Suisse fait partie des trois pays au monde où TuneIn est le plus populaire, souligne à Genève Julien Venetz. Le rapport entre le nombre d'utilisateurs uniques par mois et la population dépasse 5%.» L'entreprise qui emploie 80 personnes a levé l'année dernière 16 millions de dollars auprès de célèbres fonds d'investissement comme Sequoia Capital ou Google Ventures. Son modèle commercial repose sur la publicité.

TuneIn a récemment enrichi son interface d'une fonctionnalité baptisée «Live», qui suggère à l'auditeur des stations qui correspondent à ses goûts. **A. H.**

MULTI ASTUCES

Intégrez Facebook dans votre navigateur

FIREFOX Vous êtes assidûment connecté à **Facebook** et vous ne voulez rien manquer des nouvelles infos ou messages de vos amis. Alors, avec le navigateur au panda roux, vous pouvez suivre en permanence ce qui se passe sur le réseau social tout en surfant sur d'autres sites. Il n'y a plus besoin d'ouvrir la page **Facebook** pour suivre les publications ou discuter avec vos amis connectés. Depuis la version 17 de **Firefox**, il vous suffit d'activer la barre **Facebook** qui s'intègre dans votre navigateur. Et cela fonctionne sur **PC** comme sur **Mac**.

Une fois **Firefox** ouvert, inscrivez la commande **about: config** *(sans espace)* dans la barre d'adresse et appuyez sur la touche **Entrée** de votre clavier. Cliquez sur le bouton **Je ferai attention, promis!** et inscrivez ensuite **social.enabled** dans le champ **Rechercher**. Double-cliquez sur l'option **social.enabled** qui s'est affichée dans l'espace en dessous pour que sa valeur passe de **false** à **true**. La barre **Facebook** surgit aussitôt dans la colonne de droite. Ne reste plus qu'à vous identifier en cliquant sur le bouton **Connexion**, entrer votre adresse électronique et votre mot de passe dans les champs respectifs, et cliquer de nouveau sur **Connexion**. Désormais vous pourrez suivre vos amis grâce cette barre qui restera affichée alors que vous surfez sur n'importe quel autre site, et les notifications s'afficheront dans cette colonne.

Eric Othon

astuces.lematin.ch
Découvrez en vidéo la marche à suivre sur ordinateur et aussi sur iPhone: http://bit.ly/podcastuces