Article publié le jeudi 9 mars 2023 sur Le Temps

Alerte sur des tentatives de piratage de comptes bancaires en Suisse

Le Centre national pour la cybersécurité lance un avertissement : les cybercriminels ont accès à des comptes bancaires, malgré des mesures de protection élevées, en incitant les victimes à leur fournir des informations. Raiffeisen est notamment concernée

Attention, danger. Les pirates informatiques ciblent de manière intensive les détenteurs de comptes bancaires en Suisse via des méthodes de plus en plus sophistiquées. Et parfois, ces tentatives réussissent et des transferts frauduleux de fonds ont lieu. Cette semaine, le Centre national pour la cybersécurité (NCSC) a émis une alerte à ce sujet, montrant comment les hackers œuvrent. Comme d'autres établissements financiers, la banque Raiffeisen est attaquée par ces pirates.

C'est dans son dernier rapport hebdomadaire que le NCSC lance un avertissement. Le centre constate une explosion des signalements de *phishing* («hameçonnage»), soit des tentatives de fraude via de faux e-mails et faux sites web: 434 signalements en décembre 2022, 541 en janvier et 676 en février. Les tentatives d'arnaque explosent, et les cybercriminels testent de nouvelles attaques, notamment en temps réel contre des banques. Non seulement les hackers parviennent à obtenir le nom d'utilisateur et le mot de passe des victimes, mais en plus arrivent à subtiliser le code de sécurité supplémentaire – un mot de passe à usage unique.

Victimes sous pression

L'arnaque débute de manière classique, en redirigeant, via un e-mail prétendument envoyé d'une banque, vers un site frauduleux ressemblant au site de la banque, où la victime va taper son nom d'utilisateur et son mot de passe. Ensuite, détaille le NCSC, les pirates ouvrent en arrière-plan le vrai site e-banking et se connectent au véritable compte. Un code s'affiche à l'écran, code que la victime doit saisir sur le lecteur de carte à côté d'elle, afin de générer un second code de sécurité. «Comme les cybercriminels ne sont pas en possession de la carte bancaire, ils doivent inciter la victime à générer ce deuxième facteur pour eux», écrit le NCSC.

Ensuite, les pirates parviennent, via d'autres étapes rapides, à accéder au compte. Ce n'est pas tout: les cybercriminels demandent encore à la victime d'indiquer son numéro de téléphone portable. «Ils pourront ainsi communiquer avec elle ultérieurement et utiliser ce biais pour l'inciter à leur fournir une nouvelle fois le deuxième facteur ou la pousser à d'autres actions irréfléchies», déplore le NCSC.

Certainement des succès

De l'argent a-t-il été ainsi volé? Le Centre national pour la cybersécurité pense que oui: «Les annonces reçues par le NCSC ne faisaient clairement référence ni à un dommage financier, ni même à un accès réussi de la part des attaquants, répond une porte-parole. Néanmoins, nous partons du principe que ce genre d'hameçonnage doit être concluant pour les auteurs, sinon cette méthode aurait été délaissée au profit d'autres plus efficaces.»

Responsable de lutte contre la fraude au sein de société de cybersécurité NetGuardians, Sandy Lavorel estime que des banques et des clients ont ainsi perdu de l'argent. «Nous bloquons très régulièrement des transactions liées à des fraudes expliquées par le NCSC. Ces dernières ne demandent pas de grandes connaissances techniques et sont lucratives pour les cyberpirates. Ce type de fraude peut être très facilement fait à grande échelle et pour un moindre coût grâce aux outils informatiques mis à la disposition de tout un chacun: site web, darkweb, tutoriel sur des plateformes comme Telegram, etc.»

Contournement possible

Est-ce à dire que la double authentification (mot de passe et code reçu) n'est plus une garantie de sécurité suffisante? «Il est très facile de contourner la double authentification en demandant directement à la victime de valider le bénéficiaire ou le paiement via un message sur l'écran, poursuit Sandy Lavorel. Très souvent, les personnes ciblées sont des hommes de plus de 60 ans. Ces personnes sont moins informées et donnent les informations directement aux fraudeurs.»

Le NCSC, de son côté, relativise: «Il n'y a pas de sécurité à 100%. Toutefois, la double authentification constitue un obstacle très important pour une attaque réussie», estime sa porte-parole. Mais attention, avertit-elle, «dans le cas décrit par NCSC, le deuxième facteur a été supprimé par ingénierie sociale. En tant que client, il est donc important de respecter les règles de base en matière d'e-banking sécurisé et de ne jamais saisir de données personnelles telles que des mots de passe ou des données de carte de crédit sur une page web sur laquelle on a cliqué via un lien dans un e-mail ou un SMS.»

Raiffeisen concernée

Sur son site, Raiffeisen donne des exemples de tentatives d'arnaque dont ont été victimes ses clients, avec des e-mails prétendument envoyés par la banque en janvier dernier. «Les cybermenaces ont augmenté ces dernières années, constate une porte-parole de la banque. On peut toutefois constater que les dommages subis par les clientes et les clients de Raiffeisen se situent à un niveau très bas grâce aux mesures de sécurité étendues. Pour des raisons de sécurité, Raiffeisen ne s'exprime pas sur les détails des cas de fraude.»

Concernant la double authentification, la banque affirme qu'il «augmente considérablement la sécurité du login et constitue un élément d'un concept de sécurité à plusieurs niveaux. Avec PhotoTAN [scan d'un code avec le téléphone, ndlr], Raiffeisen propose une procédure de login sûre qui, outre une connexion sécurisée au login, permet également, selon le paiement, de signer certaines transactions.»

Prudence à plusieurs niveaux

Que faire pour tenter de déjouer ces tentatives de fraude? «Il est important que les clients vérifient la plausibilité des données affichées pendant la connexion, ainsi que lors de la signature de la transaction, et ne les valident que si toutes les données sont correctes à 100%», conseille la porte-parole de Raiffeisen. De son côté, l'expert de NetGuardians suggère que soient lancées des campagnes de prévention «plus ciblées, plus cohérentes et qui ont plus d'impact». Sandy Lavorel poursuit: «Les banques doivent se doter de solutions contre la fraude innovantes qui puissent détecter les transactions financières résultant de ces cas d'hameçonnage. De plus, il faut une meilleure collaboration: les banques à l'origine et à la réception des transactions doivent collaborer plus étroitement pour mieux comprendre où l'argent est envoyé et pourquoi. Cela signifie créer un réseau d'intelligence basé sur le partage de signaux sous forme de métadonnées, et en temps réel.»

De son côté, le NCSC insiste, sur son site, sur le fait de ne jamais saisir des données personnelles telles que des mots de passe ou des données de carte de crédit sur une page web à laquelle l'on a

accédé en cliquant sur un lien dans un courriel ou un SMS. Le NCSC appelle aussi à la méfiance vis-à-vis des «courriels qui essaient de piquer votre curiosité ou qui exigent une action de votre part, en vous menaçant sinon de conséquences». Autre élément important: aucune banque ni aucun établissement de cartes de crédit n'envoient un courriel pour vous demander de modifier des mots de passe ou de vérifier les données de votre carte de crédit, assure le NCSC.