

Des hackers s'attaquent aux clients de 12 banques suisses

Des cybercriminels piratent depuis peu les comptes en ligne des clients de 12 banques suisses grâce à un virus nommé Retefe.

Des pirates informatiques se sont lancés, depuis peu, dans une attaque d'envergure contre les comptes e-banking de douze banques suisses. Leurs méthodes sont perfides et laissent peu de traces, avertit Switch.

Le virus, de type cheval de Troie, a été nommé Retefe, a indiqué mardi Serge Droz, expert en sécurité auprès de l'organisme qui administre les noms de domaines en Suisse. Il confirmait une information parue sur le site Internet de la *Handelszeitung*. C'est l'entreprise de sécurité informatique Trend Mikro qui a rendu publique l'information sur l'attaque.

Le client de banque ouvre un spam - un courrier électronique indésirable - qui libère le virus. Le programme malicieux s'efface, une fois que l'infection a réussi. Aussitôt que le client ouvre une session e-banking, il est redirigé sur un mauvais serveur, sur lequel apparaît une copie de page Internet de sa banque. Le client entre alors ses informations de sécurité, qui sont désormais en main des malfaiteurs.

Application manipulée

Il est ensuite invité à installer une fausse application sur son smartphone, qui transfère le numéro de transaction mobile (mTan), reçu par SMS, aux hackers. Ceux-ci ont ensuite tout le contrôle sur les accès e-banking de leur victime.

Serge Droz n'était pas en mesure de révéler les noms de banques concernées. La liste change régulièrement. En Suisse, ce sont surtout les principales banques de détail qui sont visées par ces attaques.

Mais les clients peuvent aisément savoir s'ils sont touchés. «Si au cours d'une session e-banking vous avez été invité à installer une application sur votre téléphone, vous êtes l'une des victimes de ces criminels», a-t-il affirmé. Dans ce cas, il convient d'informer sa banque au plus vite, pour stopper d'éventuelles transactions abusives.

Un cas particulier

Le cas est particulier, car ce ne sont que des banques en Suisse, en Autriche et au Japon qui sont touchées. Et l'attaque est très difficile à détecter. «Le virus ne produit que deux modifications, qui ne sont qu'à peine visibles par un œil averti», a expliqué Serge Droz. Il ne laisse presque aucune trace sur l'ordinateur infecté et les logiciels antivirus ne le repèrent pas.

«Nous surveillons ce cheval de Troie depuis qu'il a fait son apparition en Suisse», fin 2013, a noté l'expert de Switch. Des analyses auraient permis de désamorcer une bonne partie du dispositif d'attaque. (ats/Newsnet)

Créé: 22.07.2014, 18h36,

<http://www.tdg.ch/economie/Des-hackers-s-attaquent-aux-clients-de-12-banques-suisses/story/16520131>

