

Attaque DNS : quand des cybercriminels remplacent une banque sur le Net

C'est probablement une attaque d'une ampleur jamais vue qu'un groupe de cybercriminels a menée contre une banque brésilienne le 22 octobre dernier. Au cours d'une après-midi, lors d'un week-end, les assaillants sont parvenus à rerouter l'intégralité du trafic online dirigé vers les services de cet établissement en direction de faux sites en leur possession. Une façon évidemment redoutablement efficace de récolter une moisson d'accès aux vrais comptes bancaires des utilisateurs.

Cette opération d'une ampleur inédite, décrite par Kaspersky, passe par une modification des enregistrements DNS de 36 services online de la banque en question. Ce qui a non seulement permis d'emmener les utilisateurs vers des sites de phishing, mais aussi de les infecter avec des malwares distribués depuis ces faux sites bancaires, afin de récolter d'autres codes d'accès (autres banques, e-mail, FTP) ou données (comme des listes de contacts Outlook ou Exchange).

Le drapeau pirate hissé pendant 5 ou 6 heures

Les chercheurs de Kaspersky pensent que les hackers sont également parvenus à rediriger toutes les transactions effectuées sur les automates bancaires ou sur les machines en points de vente vers leurs propres serveurs, collectant ainsi les données des cartes de crédit de toute personne utilisant ce type de services un dimanche après-midi. La prise de contrôle aurait duré entre 5 et 6 heures, selon Dmitry Bestuzhev, un des chercheurs qui a suivi l'attaque en temps réel, après avoir détecté l'infection d'un client de la banque

par un malware injecté depuis un domaine semblant appartenir à l'établissement financier. La banque ne serait parvenue à bloquer l'attaque qu'après avoir repris le contrôle de ses enregistrements DNS, via des contacts avec son prestataire spécialisé.

Le nom de l'établissement concerné n'a pas été dévoilé, mais l'éditeur russe assure qu'il s'agit d'un établissement de premier plan, comptant des centaines de succursales, des activités aux Etats-Unis et quelque 5 millions de clients. Au-delà de l'imitation des sites bancaires, l'attaque impressionne surtout par le détournement DNS à grande échelle. Rappelons que ce protocole central d'Internet fait le lien entre les URL (comme www.silicon.fr) et les adresses IP.

Des certificats émis au nom de la banque

Pour mener à bien leur attaque, les hackers auraient compromis le compte de la banque auprès du registrar Registro.br, un prestataire dépendant du gestionnaire du .br (NIC.br) et qui servait aussi de gestionnaire DNS pour l'établissement ciblé. En prenant le contrôle de ce compte, les assaillants seraient parvenus à modifier simultanément tous les enregistrements des services dépendant de l'entreprise et à les rediriger vers des serveurs qu'ils contrôlaient, des machines hébergées sur la plateforme Cloud de Google.

Selon Kaspersky, ces faux sites possédaient même des certificats émis au nom de la banque, tant et si bien que les clients avaient réellement l'impression de surfer sur les sites légitimes de leur établissement (avec le petit cadenas vert et le nom de la banque affichés par le navigateur). L'éditeur russe assure que ces certificats ont été émis 6 mois avant l'attaque par Let'sEncrypt, une autorité de certification gratuite mise sur pied afin d'accélérer l'adoption du HTTPS. Dans un entretien avec *Wired*, le

fondateur de Let's Encrypt assure que la délivrance de ces certificats ne constitue en rien une erreur de la part de l'autorité, dans la mesure où les cybercriminels pouvaient prouver qu'ils contrôlaient bien le domaine concerné.

Ingénierie sociale ou piratage du prestataire DNS ?

Kaspersky ne se prononce pas sur le nombre de clients qui ont pu être victimes de cette arnaque. Et le sont peut-être encore via le malware distribué par les cybercriminels. Mais l'éditeur estime toutefois que cette attaque coordonnée a pu toucher des centaines de milliers, voire des millions de clients. *« Nous ne savons réellement pas ce qui a causé le plus de tord : le malware, le phishing, le piratage des points de vente ou celui des distributeurs de billets »*, dit Bestuzhev.

Reste des questions quant à l'origine de la compromission du compte de la banque auprès de son prestataire DNS. Est-ce un hameçonnage ciblé qui a permis aux cybercriminels de récupérer les codes d'accès du gestionnaire de ce service au sein de l'établissement financier ? Ou un piratage de NIC.br ? Kaspersky pointe sur un étrange billet de [blog](#) publié le 18 janvier par le gestionnaire du .br qui admet une vulnérabilité sur son site et parle *« d'épisodes récents ayant des répercussions majeures et mettant en œuvre des changements de serveurs DNS »*. NIC.br assure toutefois que son site n'a pas été hacké et pointe vers une attaque par ingénierie sociale, contre les titulaires légitimes des comptes sur ses services. Le gestionnaire DNS conteste également le fait que 36 enregistrements DNS aient été modifiés.

Quelle que soit l'origine de l'attaque, la mésaventure de la banque brésilienne illustre le caractère critique du service DNS, capable, en cas de compromission, de rendre toute autre mesure de sécurité totalement inutile. Cette attaque prouve

encore le besoin de protéger solidement les accès au service de gestion du DNS – au minimum via une double authentification – et la fonction permettant de modifier les enregistrements.

Lire également

[Des pirates chinois attaquent les entreprises via les services Cloud](#)

[Un groupe de pirates menace de réinitialiser 200 millions d'iPhone](#)

[2016, l'année des vols de données massifs](#)

Photo : slimmer_jimmer via [VisualHunt](#) / [CC BY-NC-ND](#)