Comment notre compte Twitter a été piraté

Comment notre compte Twitter a été piraté

Après une première série de tentatives, des pirates liés au régime syrien ont pris le contrôle de notre compte Twitter, dans la nuit de mardi à mercredi. Nous avons tenté de reconstituer leur cheminement.

Le Monde | 24.01.2015 à 07h28 • Mis à jour le 24.01.2015 à 19h01 | Par Martin Untersinger et Damien Leloup

On y a cru. Mardi 20 janvier au soir, nous pensions avoir évité le pire : après une série d'attaques informatiques variées menées par l'Armée électronique syrienne, nous pensions avoir coupé tous les accès par lesquels les pirates avaient pu s'infiltrer. Nous avions tort.

Peu avant une heure du matin, un coup de fil d'un confrère réveille plusieurs personnes de la rédaction : le compte Twitter du Monde diffuse à nos trois millions d'abonnés des messages anti-Charlie Hebdo. Ce détournement est signé. L'un des messages arbore l'aigle et le drapeau syriens, accompagnés d'une phrase laconique : « L'armée électronique syrienne était ici. »

Durant quarante minutes, ce groupe de hackeurs soutenant le régime de Bachar Al-Assad gardent le contrôle de notre compte, allant jusqu'à changer la biographie de

présentation (« compte piraté par @Official_SEA16 »). Quelques coups de téléphone aux responsables de Twitter permettent de suspendre le compte et d'en reprendre la main.

Mais le mal est fait : nous nous sommes fait avoir, en raison d'attaques qui avaient débuté durant le week-end. La première a pris la forme de deux vagues successives de courriels piégés. Ils ont été envoyés depuis l'extérieur et étaient camouflés pour faire croire au destinataire qu'ils émanaient de journalistes et de rédacteurs en chef. Ces e-mails contenaient un simple lien en apparence inoffensif, mais qui renvoyait vers de fausses pages de connexion à nos messageries électroniques. Les attaquants avaient bien fait leurs devoirs : chaque victime avait droit à sa propre page, personnalisée la plupart du temps avec son adresse courriel, déjà pré-remplie, et parfois sa photo.

UN APPÂT ASTUCIEUX ET GROSSIER

Cette technique, communément appelée « hameçonnage », est vieille comme le Web. Dans notre cas, elle s'est doublée d'une bonne couche de ce que l'on appelle « l'ingénierie sociale ». Avant de lancer leur opération, les hackeurs ont vraisemblablement fait quelques recherches, dans le but de cibler précisément les personnes qui pouvaient détenir les mots

de passe de nos comptes sur les réseaux sociaux. Ils se sont donc fait passer pour certains de leurs plus proches collègues, et se sont attaqués à un système non pas en recourant à des technologies très élaborées, mais en ciblant ce qui reste toujours le point le plus faible : l'humain.

L'appât était astucieux, tout en étant grossier. Il supposait qu'un destinataire entrerait ses identifiants de connexion après avoir cliqué sur un lien vers la BBC ou YouTube, ce qui n'est pas normal. Mais lorsque le navigateur comporte déjà quinze onglets différents, que l'on ouvre le lien « pour plus tard » sans le regarder directement, on ne se souvient plus nécessairement de quelle page correspondait à quoi… Surtout si l'on ne s'attend pas à être visé personnellement. Tant que l'on ne s'est pas fait piéger, on croit que le piratage, c'est un peu comme les maladies honteuses ou les accidents idiots : « ça n'arrive qu'aux autres ».

Lundi vers 10 heures, l'un des journalistes ayant accès au compte Twitter du Monde reçoit un étrange message d'une consœur lui demandant, dans un mauvais français, le mot de passe du compte. Nous comprenons alors que sa boîte e-mail a été piratée. D'autres l'ont peut-être été : nous changeons alors en catastrophe les mots de passe permettant d'accéder à nos comptes sur les réseaux sociaux et aux différentes boîtes.

Nous avons eu une grosse frayeur, mais nous pensons alors avoir évité le pire. La boîte e-mail piratée de notre journaliste ne contenait pas de mots de passe. Ses archives n'ont pas été téléchargées, et elle ne semble pas avoir envoyé aucun autre message douteux. En revanche, un paramètre peu connu, qui permet d'envoyer automatiquement une copie de tous les e-mails reçus et envoyés à un autre destinataire, a été modifié, dans le but d'envoyer les messages à une adresse inconnue.

Durant la journée, l'analyse des messages frauduleux nous permet de remonter en partie la trace des hackeurs, et de prévenir deux administrateurs aux Etats-Unis que leurs machines sont squattées par des pirates qui s'en servent pour tenter de nous piéger.

En fin d'après-midi, nouvel incident. Des brouillons d'articles se multiplient dans notre outil de publication. Intitulés, pour la plupart, « piraté par l'Armée électronique syrienne », ils ne laissent guère de place au doute : les pirates sont parvenus à pénétrer notre outil de publication. Il n'y avait pas trente-six moyens d'y arriver : les hackeurs ont eu accès aux boîtes e-mail des personnes concernées…

Nous pensions que deux personnes avaient été infectées, nous comprenons désormais qu'elles sont en fait plus nombreuses. Ne sachant pas combien exactement, une décision

radicale est prise en extrême urgence. Les gens détalent dans les couloirs du journal avec un double objectif : désactiver immédiatement notre outil de publication et conserver un maximum de traces possibles de cette intrusion.

Dans un second temps, décision est prise de procéder à une réinitialisation générale de tous les mots de passe de toutes les boîtes de l'entreprise. Le remède s'avère assez lourd de conséquences : par définition, il est impossible de prévenir l'ensemble des salariés, par e-mail, que leur accès va être coupé. Les téléphones portables chauffent, bombardés de messages de journalistes inquiets de ne plus avoir d'accès et qui pensent être victimes d'un piratage.

Un repérage passé inaperçu

A peu près au même moment, les serveurs du Monde sont visés par de très nombreuses fausses connexions, une attaque dite de « déni de service » qui vise à paralyser notre site. Ce dernier est considérablement ralenti mais tient bon. Dans la rédaction et au service informatique, ce « changement d'arme » est d'abord interprété comme un bon signe : frustrés de ne pas avoir réussi à publier leurs messages, les attaquants s'en remettent à une méthode beaucoup plus brutale. Nous apprendrons plus tard que les pirates ont prévu depuis longtemps cette attaque par déni de service : dès le milieu de la journée, ils avaient procédé à une première salve, mais de très faible intensité, destinée à évaluer nos défenses. Ce repérage est passé inaperçu.

Au moment où nous faisons face à cette nouvelle attaque, il y a une autre chose que nous ignorons : les pirates n'ont pas renoncé à prendre le contrôle de notre compte Twitter. Le dimanche, ils ont en effet trouvé la trace d'un ancien compte Gmail resté lié au compte Twitter du Monde.fr. Mieux, ils ont également mis la main sur son mot de passe. Pendant la journée de dimanche, ils tentent à plusieurs reprises de s'y connecter. La provenance de ces connexions déclenche cependant un mécanisme de sécurité de Google, qui leur soumet

la question de sécurité du compte en question, ce qui les empêche de pénétrer dans la boîte e-mail.

Cela a découragé les pirates, qui ont abandonné provisoirement cette piste et décidé de lancer une deuxième vague de courriels d'hameçonnage. Après avoir échoué à publier leur message directement sur notre site lundi soir, ils retentent leur chance sur notre compte Twitter dans la nuit de mardi à mercredi. Ils réussissent, à minuit et demie, à résoudre la question de sécurité de l'adresse e-mail liée à ce dernier. Sur Twitter, ils n'ont plus qu'à cliquer sur le lien qui leur permet de choisir un nouveau mot de passe pour le compte du Monde, et en prendre le contrôle.

« L'interface chaise-clavier »

Ne tournons pas autour du pot : si notre compte Twitter a été piraté, c'est parce que nous avons commis des erreurs. Tout d'abord, ce vieux compte e-mail n'aurait jamais dû y être associé, et aurait dû être mieux protégé. Surtout, nous aurions dû activer la double authentification sur notre compte Twitter, ce système qui nécessite, pour se connecter, d'entrer non seulement un mot de passe mais aussi un code secret envoyé par SMS.

Un dicton populaire dans les services informatiques veut que « la plus grande des failles de sécurité, c'est l'interface chaise-clavier » : à savoir, l'utilisateur. Chacun de nous fait des erreurs, en somme. Le piratage qui nous a touchés n'était pas d'une grande sophistication technique, mais a été mené par des individus déterminés et bien renseignés qui ont su tirer parti de nos erreurs.

La bonne nouvelle, c'est que les pirates, eux aussi, font des erreurs. Ceux qui ont détourné notre compte Twitter ont camouflé l'adresse de leurs ordinateurs tout au long de leurs attaques. Dans tous les cas sauf un : la trace d'une connexion au compte Gmail détourné mène directement à Damas.

Article original : http://www.lemonde.fr/pixels/article/2015/01/24/comment-notre-compte-twitter-a-ete-pirate_4562506_4408996.html