Nos amis sont ses amis

Yves Eudes

En cette fin de matinée, Yves Lavallée, employé de bureau parisien, décide de s'accorder une petite récréation et se connecte sur sa page Facebook. Il va peut-être y trouver des messages de sa bande de copains, ou un quiz amusant à faire en cinq minutes… Cette fois, il découvre un nouveau message : *« Exclu ! Les photos de Nicolas et de Carla nus, à la plage ! »* Il a été envoyé par une jeune femme qu'il ne connaît pas, et qu'il a acceptée comme *« amie Facebook »* parce qu'elle est jolie. C'est peut-être un attrape-nigaud ou une opération de marketing viral, mais l'adresse du site photos semble rassurante : http://apps.facebook.com/sarkozynu. On reste dans l'univers de Facebook, qui a la réputation d'être surveillé et civilisé. Yves clique sur le lien, machinalement.

En fait, Nicolas et Carla ne sont pas nus sur les photos, seulement en maillot de bain. Encore un canular sans intérêt, Yves hausse les épaules et passe à autre chose. Quelques secondes plus tard, il a oublié l'incident. C'est voulu, car en réalité, il vient de lui arriver quelque chose dont il doit tout ignorer. En même temps que les photos, il a téléchargé, à son insu, un logiciel pirate qui a recopié toutes les données personnelles de son compte Facebook, toutes ses photos publiques et privées, tous ses messages reçus et envoyés – y compris ses coordonnées, officiellement protégées par le système de confidentialité proposé par le site. Puis, en une fraction de seconde, tout a été envoyé sur un serveur appartenant à l'expéditeur des photos, qui n'est pas une jolie jeune femme, mais un hacker expérimenté.

Yves ignore aussi que le logiciel malveillant, contenant un virus très sophistiqué, s'est emparé de sa liste d'amis et leur a automatiquement envoyé le message, en se faisant passer pour lui. Or, statistiquement, on peut prévoir que la moitié des amis d'Yves vont cliquer sur le lien et se faire contaminer à leur tour. Parmi eux, Damien Lamontagne, qui a créé un compte Facebook sécurisé, accessible seulement à ses amis, choisis un par un, et qui se croit donc protégé. Damien va cliquer sur le lien sans réfléchir, car l'application est recommandée par son ami Yves, en qui il a confiance. Ainsi, le pirate, qui n'a aucun contact avec Damien et ne sait même pas qu'il existe, va recevoir automatiquement toutes ses données, publiques et privées.

Dès lors, la progression du virus est exponentielle : au rythme où les internautes cliquent sur les quiz et les photos qui leur sont proposés, il peut siphonner des centaines de milliers de comptes dès le premier jour – et ainsi de suite. Le pirate va pouvoir constituer sa propre base de données sur le contenu du réseau social.

Par le jeu des amis communs, si Damien néglige le message à sa première apparition, il va le recevoir plusieurs fois, provenant d'amis différents : il finira par cliquer, de guerre lasse. En plus des données individuelles, le pirate va répertorier les réseaux de contacts qui se créent sur Facebook. Or, c'est bien connu, dis-moi qui tu fréquentes, je te dirai qui tu es.

Par ailleurs, le pirate peut paramétrer son virus pour qu'il se propage au-delà des réseaux d'amis existants : une fois infecté, le compte va accepter automatiquement toutes les demandes d'amis, sans aucun filtrage. Il peut aussi activer un système de mise à jour automatique : les comptes d'Yves et de Damien seront pillés à date fixe, tous les mois ou toutes les cinq minutes.

En réalité, Yves Lavallée et Damien Lamontagne n'existent pas. Ces deux comptes ont été créés pour tester l'efficacité du virus, car si l'expérience avait été réalisée sur un compte réel avec de vrais amis, il aurait infecté d'innombrables comptes avant que les systèmes d'alerte de Facebook ne le repèrent. Cette attaque a été imaginée et réalisée par John Jean (c'est son vrai nom), un Français âgé de 26 ans. M. Jean est le patron d'une petite société de sécurité informatique baptisée Wargan, qu'il a fondée quand il avait 20 ans, à Amiens (Somme), sa ville natale. Avec ses six employés, il occupe un petit appartement transformé en bureau dans le centre-ville, en face de la mairie.

John Jean affirme que, dans cette affaire, ses motivations sont purement professionnelles, et presque altruistes : *« Facebook est très décrié, notamment sur sa gestion des paramètres de confidentialité. Alors j'ai eu l'idée d'effectuer un audit sur leur site, afin de m'assurer que les données des internautes étaient bien en sécurité. Après tout, les patrons de Facebook répètent sans arrêt que tout est parfaitement sécurisé, alors pourquoi pas vérifier… »*

En août 2010, après quelques recherches, John Jean découvre une faille de sécurité dans l'un des programmes permettant de faire fonctionner le site sur les mobiles. Pour simplifier, il peut s'introduire dans un profil en supprimant le numéro d'identification affiché à la fin de l'adresse Facebook, et en le remplaçant par une balise autorisant le téléchargement d'un logiciel. Il parvient aussi à utiliser l'adresse de confiance Apps.facebook.com, tout en dirigeant l'internaute vers un serveur extérieur.

Puis John Jean se lance dans l'écriture du logiciel proprement dit : *« Il fait environ 500 lignes de code, ce qui représente sept jours de travail pour un professionnel de mon niveau. La partie la plus complexe à mettre au point a été la fonction réplication, permettant d'infecter automatiquement les amis d'amis. »*

Dès qu'il a testé l'efficacité de son virus et de son mode de pénétration, John Jean, très loyalement, prévient le service de sécurité de Facebook : *« D'abord, ils m'ont répondu qu'ils allaient enquêter. Une semaine plus tard, je les ai relancés, et au bout de quinze jours, j'ai constaté que la faille était colmatée. Ils ne m'ont pas donné de récompense, juste un petit remerciement, affiché sur un site Internet. »* John Jean se charge alors d'annoncer lui-même son exploit sur différents sites professionnels, et obtient en retour quelques demandes de devis pour des contrats de sécurité : *« Mais attention*, précise-t-il*, je n'ai livré à personne le code de mon application, ça pourrait suffire à mettre Facebook par terre. Je préfère maîtriser. »*

Sur sa lancée, deux mois plus tard, John Jean découvre une nouvelle faille de sécurité, assez similaire, située cette fois dans les logiciels permettant à Facebook de gérer les connexions via un écran tactile. Malgré les pressions constantes des utilisateurs, Facebook a du mal à améliorer les systèmes de protection de la vie privée de ses utilisateurs, peut-être parce que son *business model* et toute sa culture d'entreprise sont orientés dans l'autre sens : l'exploitation des données personnelles à des fins commerciales, et le partage de ce trésor de guerre avec des partenaires extérieurs.

Le captage de données n'est qu'un avant-goût de ce que John Jean affirme pouvoir faire avec les failles du site. Il a mis au point d'autres pièges, encore plus dévastateurs. Exemple : quand l'internaute clique sur un lien pour accéder à une photo ou à un quiz, il voit une fenêtre ressemblant en tout point à une page officielle de Facebook, qui lui demande de confirmer son intention en retapant son nom et son mot de passe. *« En fait, il est cuit d'avance*, explique John Jean. *Soit il accepte d'entrer son mot de passe, et je l'obtiens directement ; soit il clique sur "annuler", mais, en fait, mon application ne revient pas en arrière, elle change carrément son mot de passe. »* Dès lors, tout devient possible. Le pirate peut désactiver le compte, le vider, le remplir de nouvelles données, et même, s'il a un peu d'imagination, se faire passer pour son propriétaire afin de détruire sa réputation ou de lancer une opération d'usurpation d'identité.

> « Après tout, les patrons de Facebook répètent sans arrêt que tout est parfaitement sécurisé, alors pourquoi pas vérifier… »
>
> **John Jean**

Bien sûr, John Jean n'est pas le seul à posséder ce type de compétences. Quand on raconte cette histoire à d'autres professionnels de la sécurité, ils la trouvent très plausible. Selon eux, Facebook est régulièrement victime d'attaques de pirates visant à voler des informations personnelles pour constituer des bases de données illicites et les revendre à des entreprises de marketing en ligne, à des spammers, à d'autres pirates, ou, dans certains pays peu respectueux des droits de l'homme, à des administrations. Cette pratique a déjà un nom : le *clickjacking* (« détournement par clic »). Comment s'en prémunir ? Un jeune chercheur français travaillant pour la société de sécurité Kaspersky, qui souhaite rester anonyme, a trouvé un remède très simple : *« Je ne suis pas sur Facebook, il y a trop de problèmes de sécurité insolubles. »*

Ses collègues, moins radicaux, utilisent Facebook dans leur vie privée et professionnelle, tout en surveillant de près les attaques visant les autres utilisateurs. Récemment, l'un d'entre eux a raconté sur son blog d'entreprise qu'il avait repéré une application de vol de mots de passe qui se propageait via la messagerie interne de Facebook. En pénétrant à son tour dans le serveur du hacker, l'expert a constaté que le programme avait subtilisé 3 000 mots de passe en vingt minutes.

Un autre hacker, très innovant, a su tirer profit de la fonction « I Like » (« J'aime ») permettant à un utilisateur de Facebook de faire savoir à ses amis qu'il a aimé un nouveau site. En suivant un lien proposant les photos des *« 101 femmes les plus belles du monde »*, l'internaute télécharge à son insu un bouton « I Like » invisible et nomade, qui va suivre son curseur partout sur l'écran. Dès qu'il se sert de sa souris, il envoie à tout le monde des messages indiquant qu'il a aimé les photos des « 101 Femmes », et proposant un lien vers le site piégé.

Installé dans son petit bureau de la place de l'Hôtel-de-Ville, John Jean tire la leçon de son test, en résumant le sort d'une victime potentielle d'une attaque sur Facebook multiple et bien menée : *« C'est juste horrible ce qui va lui arriver, et c'est sans limite. »* A présent, il envisage de faire une expérience du même genre sur Twitter. ■

> John Jean, un jeune Français de 26 ans, a mis au point un logiciel qui peut s'emparer de toutes les données personnelles des utilisateurs de Facebook. Son but : démontrer que la confidentialité n'est pas garantie sur le réseau social

AMÉLIE FONTAINE