

Facebook – Une nouvelle faille de sécurité

George Lucian Petre

Chef d'équipe d'analyse des menaces - BitDefender, Bucarest, Roumanie 062204

glpetre@bitdefender.com

Résumé – En tant que réseau social le plus populaire à l'heure actuelle, ayant enregistré l'an dernier un accroissement impressionnant, Facebook est récemment devenu le théâtre d'attaques sophistiquées en termes de manipulation et de distribution à grande échelle de spam agressif et de malware. Cet article passe en revue les attaques de hameçonnage, spam et autres manipulations lancées contre Facebook au cours de l'an dernier. Il explique également comment les données personnelles des utilisateurs sont mises en danger par l'intermédiaire des jeux. La dernière partie de l'article relate une expérience qui illustre à quel point les utilisateurs sont enclins à se précipiter sans réfléchir pour ajouter des amis inconnus à leur profil, rejoindre des groupes inconnus ou devenir fans de pages dangereuses.

Mots clés – Facebook, Hameçonnage, Spam, Manipulation sociale, Malware, Menaces

I. INTRODUCTION

D'après les statistiques publiées sur son site [1], Facebook comptait en janvier 2010 plus de 350 millions de membres actifs dans le monde, soit un nombre supérieur à la population des Etats-Unis, et représentant 5,14 % de la population mondiale et 20,18 % des utilisateurs d'Internet dans le monde [2]. Et plus de 700.000 professionnels ont une page sur Facebook. Avec un tel nombre d'utilisateurs individuels ou professionnels, il est possible d'affirmer sans se tromper que Facebook constitue une cible idéale pour des attaquants spécialisés dans les projets de manipulation sociale.

Notre atelier 2008 sur le spam à la Conférence sur le spam [2] était axé sur l'analyse des menaces pesant sur les réseaux sociaux, à un moment où il était encore difficile d'identifier les attaques au sein du réseau Facebook, et même de donner des exemples d'attaques simplistes. Aujourd'hui nous pouvons facilement identifier les campagnes de spam, les variantes de malware visant les utilisateurs de Facebook (KoobFace), les campagnes de hameçonnage destinées à récupérer des comptes Facebook ou récolter des dons prétendument destinés à réparer des désastres comme ceux provoqués par le tremblement de terre d'Haïti.

II. LES JEUX SOCIAUX, UN ACCÈS AUX UTILISATEURS

La seconde moitié de 2009 a enregistré l'apparition d'un nombre considérable de jeux sociaux, comme Farmville, Mafia Wars, Castel Age et d'autres. Pour briller à ces jeux, il est nécessaire d'avoir le plus grand nombre d'amis possible. C'est la raison pour laquelle, comme le montre la Figure 1, nous avons trouvé un grand nombre de groupes conçus pour réunir instantanément une immense quantité d'amis adeptes de ces pratiques.

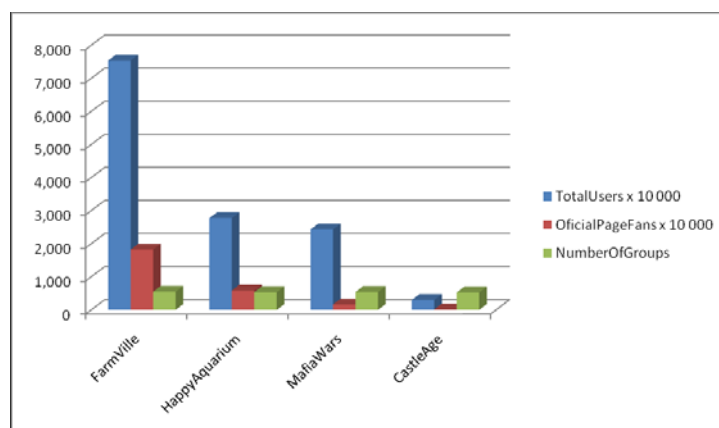


Fig. 1 – Diagramme comparatif des jeux les plus populaires sur Facebook, indiquant le nombre d'utilisateurs, le nombre de fans sur la page principale et le nombre de groupes qui leur sont dédiés.

Ces groupes sont pour les spambots le terrain idéal pour s'introduire dans des listes d'utilisateurs amis. Pour mieux comprendre comment ils fonctionnent, nous avons rejoint quelques-uns de ces groupes en utilisant un profil factice sur Facebook. Nous avons choisi Farmville parce qu'il est le jeu le plus populaire sur Facebook. Nous nous sommes inscrits à plusieurs groupes et avons ajouté le profil à notre liste d'amis avec une « image chaude » qui affichait sur le mur du groupe des messages tels que « ajoutez-moi comme voisin ». Après l'ajout de notre profil, nous avons reçu un message de « Bienvenue » auquel nous avons répondu. Et nous avons ensuite reçu un lien vers un site web de discussions vidéo. Même si ce scénario est courant dans les campagnes de spam électronique, la situation décrite présente quelques caractères particuliers :

- C'est l'utilisateur qui a ajouté le spammer à son profil, et non pas l'inverse. C'est la raison pour laquelle l'acte du spammeur ne constitue pas un abus, et son compte ne peut donc pas être supprimé.

- Le spambot commence par envoyer un message de bienvenue. C'est une stratégie destinée à gagner la confiance de l'utilisateur.

- Finalement, une fois obtenue la réponse de l'utilisateur, le lien vers le site web de discussions vidéo est envoyé par l'intermédiaire d'une url raccourcie, qui ne permet pas à l'utilisateur de voir la destination finale de la page jusqu'à ce qu'il clique sur le lien.

- Les photos et les détails du profil sont destinés à donner au spambot un aspect plus « humain ».

III. CANULARS ET ESCROQUERIES A LA CHARITE

Les vieux canulars du style « Si vous ne faites pas suivre ce message, Yahoo supprimera votre compte » sont désormais moins autoritaires. « NON, JE NE PAIERAI PAS 3,99 EUROS PAR MOIS POUR UTILISER FACEBOOK A PARTIR DU 9 JUILLET 2010 ! » est un groupe qui compte 888.594 membres. Plus de 500 groupes ont repris l'idée et discuté des coûts et des dates à laquelle les comptes sur Facebook allaient devenir payants. Etant donnée l'ampleur du phénomène, Facebook a été contraint de démentir ces rumeurs dans un important quotidien [4].

Si les canulars ont tendance à être plus amusants que dangereux, il existe en revanche des escroqueries potentiellement redoutables, fondées sur des appels à la charité. Le tremblement de terre d'Haïti a provoqué un fort élan de compassion qui s'est traduit par des dons d'un montant considérable dans le monde entier. Ce qui a provoqué le développement d'une quantité de tentatives de hameçonnage, et un grand nombre d'applications et de pages de Facebook ont commencé à se promouvoir en utilisant l'idée de « dons à Haïti ».

L'un des exemples les plus intéressants concerne un groupe de Facebook qui prétendait faire un don de 0,01 dollar chaque fois qu'un utilisateur deviendrait un fan de cette page. En 5 jours seulement la page a atteint le nombre stupéfiant de 2 millions de fans. Un grand nombre de liens contenant du spam ont été fournis aux utilisateurs par l'intermédiaire de cette page. Après avoir atteint ces 2 millions de fans, la page a été fermée pour abus.

IV. HAMECONNAGE DE COMPTES FACEBOOK

Fin octobre 2009, nos adresses « factices » ont été la cible d'une attaque massive de hameçonnage destinée à récupérer les identités d'utilisateurs de Facebook. L'attaque était même encore plus perverse car, en plus du hameçonnage, elle distribuait aussi une version de Zbot [5]. Deux méthodes de distribution sont utilisées :

- en tant que pièce jointe à un courrier électronique
- en tant qu'utilitaire fourni après que l'utilisateur se soit connecté au faux site Facebook. Cette catégorie d'attaques de hameçonnage frappe dans deux directions : d'un côté le spambot distribue du malware et pratique le hameçonnage via le courrier électronique, de l'autre le vol des données des comptes Facebook, comme nous avons pu le constater, entraîne le postage de liens vers du malware et du spam dans les profils des utilisateurs.

V. MALWARE SUR FACEBOOK

Une quantité considérable de vers a été massivement distribuée par l'intermédiaire du mur de Facebook. La méthode était simple mais efficace. En utilisant des comptes Facebook hameçonnés, les attaquants postaient un lien malveillant accompagné d'une image provocatrice et d'un message accrocheur. Parmi les exemples : « Tu veux voir quelque chose d'excitant !?? » ou « Mon ancienne copine m'a trompé. Je me venge ! ». Certains de ces vers se contentaient de poster des entrées gênantes à tous les utilisateurs de Facebook connectés en utilisant la fonction de Partage, d'autres distribuaient du malware par ce moyen.

Aussi primaire que cela paraisse, la tendance à cliquer en confiance sur des liens provenant d'amis est beaucoup plus forte qu'en ce qui concerne le spam électronique.

VI. KOOFACE – UN MALWARE REVOLUTIONNAIRE

Koobface a été le premier malware massivement distribué, spécialement conçu pour atteindre les réseaux sociaux. Koobface comporte de nombreux modules, dont l'un est destiné à la propagation sur ces réseaux. La clé du succès de Koobface est le vol de réputation. Un utilisateur infecté commence à poster des liens vers un faux lien YouTube. Le lien pointe vers un autre ordinateur infecté par Koobface, ce qui lance un autre composant du malware, appelé le téléchargeur. La Figure 2 illustre le mode d'infection de Koobface.

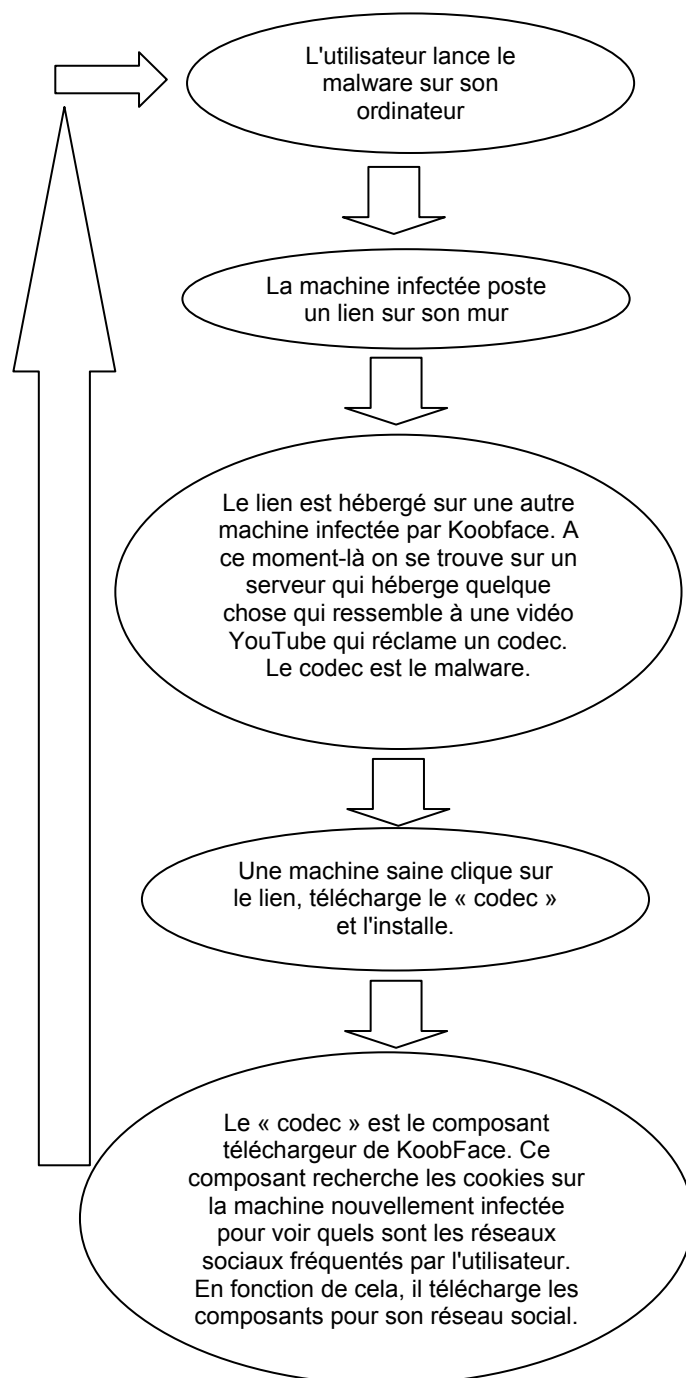


Fig. 2 – Comment KookFace se diffuse sur les réseaux sociaux

VII. EXPERIENCE SUR LA SOUMISSION DES UTILISATEURS

Une des principales raisons du succès de la manipulation des utilisateurs des réseaux sociaux réside dans le fait que les attaquants sont facilement admis dans le cercle des personnes de confiance. Nous avons conduit une expérience destinée à observer et analyser comment les utilisateurs de Facebook se laissent aussi facilement tromper et ajoutent des inconnus à leur liste d'amis.

Nous avons créé les types de comptes suivants : un profil sans image et contenant le moins de détails possible (profil 1), un profil avec une image et quelques détails (profil 2) et un autre avec de nombreux détails et images (profil 3). Avec chacun des ces profils nous avons rejoint quelques groupes d'intérêt général pour nous faire quelques amis : « Je suis de New York », « BMW », « JE SUIS ACCRO DE FAMILY GUY », « Le chocolat = J'aime ♥ !! ».

Notre première tentative a été assez réussie sans effort particulier. Une heure seulement après avoir commencé à ajouter des gens à chaque profil, nous avons 23 connections pour le profil 1, 47 pour le profil 2 et 53 pour le profil 3.

Nous avons alors rejoint des groupes de jeux sociaux et commencé à ajouter des amis. A partir de là, nous avons obtenu encore plus de succès. Au bout du compte, après 24 heures d'observation des 3 profils, les statistiques ont donné 85 pour le premier, 108 pour le second et 111 pour le troisième.

La troisième étape a consisté à ajouter des « amis communs ». La chance a encore été de notre côté puisque plus de 50 % des amis communs se sont connectés à notre profil.

Dans la dernière phase de l'expérience, nous avons posté une url bit.ly sans texte dans chacun des 3 profils et examiné combien de gens utilisaient ce lien. Le résultat a montré qu'environ 24 % des amis du profil concerné suivaient le lien, même s'ils n'avaient aucune indication sur sa destination ni sur son origine.

VIII. CONCLUSIONS

Ce panorama des menaces qu'affrontent Facebook et ses utilisateurs montre que les attaques qui ont débuté en 2008 sont devenues plus sophistiquées que jamais.

Comme l'a montré l'expérience concernant l'acceptation, les utilisateurs sont plus enclins à intégrer des spammers dans leur liste d'amis lorsqu'ils se trouvent dans des réseaux sociaux plutôt que dans d'autres environnements de communication en ligne. De ce fait, le spam et la manipulation sociale s'exerçant sur les réseaux sociaux sont plus efficaces que le spam ou les escroqueries véhiculés par courrier électronique.

De plus, nous avons constaté que les utilisateurs des réseaux sociaux se laissent facilement convaincre d'ajouter des spammers à leur profil.

En conclusion, nous pouvons dire qu'en tant que réseau social le plus populaire du moment Facebook est aussi le plus vulnérable à ce type d'attaques.

REFERENCES

- [1] *Facebook Statistics Page*
<http://www.facebook.com/press/info.php?statistics>
- [2] *Internet World Stats*
<http://www.internetworldstats.com/stats.htm>
- [3] Cosoi C. , Petre G. – Spam 2.0 (Workshop) – MIT Spam Conference 2008, Cambridge, MA, USA
- [4] *Telegraph*
<http://www.telegraph.co.uk/technology/facebook/6973757/Facebook-dismisses-rumours-of-charging-plans.html>
- [5] *ZBot Trojan Explained* <http://www.bitdefender.com/VIRUS-1000561-en--Trojan.Spy.ZBot.EHE.html>
- [6] *The real face of Koobface* – J. Baltazar, J. Costoya, R. Flores, Trend Micro Threat Research
- [7] *Is Britney Spears Spam?* - A. Zinman, J. Donath - CEAS 2007 – Fourth Conference on Email and Anti-Spam, August 2-3, 2007, Mountain View, California USA
- [8] *Brazen Black Hats: How we fight online fraud in a socially networked world* – V. Sharma- VB 2009, Genève, Suisse
- [9] *Socialnetworking: or, the friend of my friend is my enemy* – A. Lee - VB 2009, Genève, Suisse
- [10] <http://fitzgerald.blog.avg.com/2009/11/new-facebook-worm-dont-click-da-button-baby.html>
- [11] <http://mashable.com/2010/01/29/facebook-revenge-worm/>