Applications Facebook : Quels Risques pour l'Entreprise ?

François-Xavier Bru[1], Guillaume Fahrner[1] et Alban Ondrejeck[2]
fx.bru(@)telecom-bretagne.eu,
guillaume.fahrner(@)telecom-bretagne.eu,
alban.ondrejeck(@)orange-ftgroup.com

[1] Mastère Spécialisé en Sécurité des Systèmes d'Information, Télécom Bretagne
[2] Orange Consulting

Résumé Les utilisateurs ont une confiance exagérée envers les réseaux sociaux qui deviennent pourtant peu à peu une cible privilégiée des attaquants. La nature même des plateformes sociales facilite la propagation de *malwares*, qui se complexifient de génération en génération. En permettant la création d'applications intégrées, les réseaux sociaux offrent aux développeurs et aux attaquants des facilités d'accès aux données des utilisateurs, et des moyens d'interaction avec leurs comptes. Nous étudierons plus particulièrement dans cet article le cas des applications Facebook, qui est l'une des plateformes les plus populaires. Ces différents risques doivent être identifiés afin d'être évalués et de pouvoir mettre en place une véritable stratégie d'intégration maîtrisée de ces outils au sein des entreprises.

Mots-clés: Applications Sociales, Évaluation des Risques, Facebook, Malwares Sociaux, Réseaux Sociaux

1 Introduction

Le concept de réseau social n'est pas récent, le sociologue John A. Barnes utilisait déjà ce terme en 1954. Son application beaucoup plus récente sur l'Internet a donné naissance à ce que l'on appelle désormais des portails communautaires. À l'origine considérés comme un simple effet de mode, force est de constater que leur utilisation fait désormais partie des habitudes de l'internaute. Leur niveau de fréquentation augmente constamment, et le contenu qu'ils proposent s'enrichit régulièrement. A l'instar des messages électroniques, les internautes utilisent quasi- quotidiennement leur plateforme favorite, à leur domicile bien entendu mais également au travail ; que ce soit en

guise de pause, ou bien comme d'un outil pour des échanges professionnels. Ces nouveaux outils se sont donc introduits dans le monde des entreprises à l'initiative des employés sans contrôle ni mesures organisationnelles. Comment sont protégées les données confidentielles qui transitent sur ces nouvelles plates-formes ? Des logiciels malveillants peuvent-ils s'introduire dans l'entreprise *via* ces réseaux sociaux ? Quels nouveaux risques cela entraine-t-il pour les systèmes d'information des sociétés ? Cette étude des vulnérabilités engendrées au sein des entreprises et pour leurs employés est menée en parallèle d'une étude d'opportunités. Ces deux études permettront d'obtenir une vue précise des risques et des opportunités liés à l'utilisation des réseaux sociaux dans les entreprises. Il ne s'agit donc pas de dénigrer ces nouveaux outils mais d'effectuer un panorama des risques pour les intégrer de façon la plus consciente et opportune au sein de nos entreprises.

2 Malwares se propageant sur les Réseaux Sociaux

Différents *malwares* se transmettent depuis quelques temps aux utilisateurs de réseaux sociaux sur l'Internet. Ces derniers connaissent une croissance fulgurante assurant une large diffusion aux logiciels malveillants qui les utilisent. Il est intéressant d'étudier la manière dont ces *malwares sociaux* se propagent sur ces réseaux communautaires, et pourquoi leurs utilisateurs sont vulnérables. De plus, les techniques évoluent : ce qui était il y a quelques années anecdotique est aujourd'hui devenu une mode.

2.1 Des Utilisateurs Vulnérables

La plupart des réseaux sociaux qui existent aujourd'hui ont dû faire face à une très forte concurrence. Ceux qui ont su attirer le plus de membres ont survécu. En effet, le nombre d'utilisateurs actifs est le critère principal permettant d'évaluer la qualité d'un réseau social, puisque ce sont eux qui créent le contenu. Ces réseaux étant donc par définition extrêmement fréquentés, de nombreux organismes spécialisés en sécurité s'y intéressent également. Ainsi, si une vulnérabilité quelconque existe, elle est souvent rapidement décelée, puis corrigée

par les équipes de développement. Une personne malveillante désirant diffuser un *malware* ne peut donc a priori pas compter sur la découverte d'une vulnérabilité technique. On constate en revanche que les utilisateurs peu avertis font confiance aux contenus diffusés sur les réseaux ; si l'internaute est désormais méfiant envers les messages électroniques, il l'est beaucoup moins envers les messages diffusés *via* ces plateformes. L'organisme spécialisé en sécurité Sophos a mis en évidence la naïveté de certains membres au travers d'études simples : des comptes utilisateurs fantaisistes sont créés sur Facebook, puis des demandes d'ajout à la liste d'amis sont émises vers des utilisateurs pris au hasard. 41% des profils contactés ont accepté la demande, laissant ainsi leurs informations personnelles (adresse électronique, adresse réelle, numéro de téléphone, date de naissance) divulguées à un parfait inconnu [1]. Cette étude montre ainsi que la majorité des utilisateurs de réseaux sociaux ne se méfient pas des personnes qui cherchent à entrer en contact avec eux.

2.2 Une Évolution Constante

Depuis la naissance des réseaux sociaux, des *malwares* circulent régulièrement sur ces plates-formes. Au départ rudimentaires, ces programmes ont beaucoup évolué et utilisent désormais au maximum les fonctionnalités offertes par ces portails pour se propager [2]. Il est possible de les classer par génération, le terme *génération* ne désignant pas un âge mais le degré d'évolution de ces *malwares*. La première génération de logiciels malveillants utilisant les réseaux sociaux pour se propager est assez primaire. On peut considérer comme *malware* de première génération ceux qui se propagent *via* un simple e-mail, dont la provenance semble être un réseau social reconnu. Bien entendu, il s'agit d'une technique de propagation de virus déjà ancienne qui consiste à falsifier l'adresse émettrice du message, insérer un logo officiel et joindre un *malware*. Pourtant, les réseaux sociaux jouent déjà un rôle puisqu'ils sont utilisés pour leur image, à laquelle les utilisateurs portent une confiance exagérée. C'est le cas du programme identifié par Sophos sous le nom W32/Autorun-AQL, imitant les notifications du réseau social Hi5.

Les *malwares* de deuxième génération utilisent les fonctionnalités de diffusion de contenu offertes par les réseaux sociaux : messages,

musiques, vidéos, etc. Des scripts malveillants sont intégrés directement dans ces contenus, de manière à ce que les utilisateurs soient infectés à leur insu. C'est par exemple le cas de JS/SpaceTalk, qui prend la forme d'un code Javascript au sein d'un film QuickTime sur le réseau MySpace pour dérober les informations du compte de la victime. De la même manière, le ver Troj/Dloadr-BPL poste des messages sur le mur du cercle d'amis de la personne infectée. Ces messages enjoignent l'utilisateur à cliquer sur un lien pour regarder une vidéo. La victime sera en fait redirigé vers une page malicieuse proposant le téléchargement et l'éxecution d'un programme qui est un Cheval de Troie.

Les *malwares* de troisième génération sont les plus complexes : ils se propagent grâce à plusieurs réseaux en utilisant au maximum les caractéristiques de chacun. Ainsi, Koobface utilise plusieurs portails communautaires pour se diffuser et se maintenir dans les systèmes d'information [3]. On citera notamment Facebook, MySpace, Twitter et Hi5. Il s'agit d'une petite révolution dans l'industrie du *malware* qui peut désormais compter sur plusieurs portails comme vecteur de propagation. Une étude de Trend Micro montre qu'il existe plusieurs modules permettant à Koobface de communiquer avec différents portails communautaires. Ces plug-ins sont téléchargeables par le composant de base du ver, lui permettant ainsi de s'adapter à sa victime. Une fois la machine infectée et les composant téléchargés, chaque module de propagation va effectuer les opérations suivantes :

- Contacter le C&C (Command & Control),
- Récupérer les messages à envoyer et les URL permettant de poster sur le(s) réseau(x),
- Diffuser les messages récupérés par e-mail, message interne et sur le mur.

Les e-mails envoyés contiennent un lien vers un site dont l'identité a été usurpée, généralement un autre portail communautaire proposant du contenu multimédia, type Youtube, qui utilise des technologies telles que Flash et Javascript pour fonctionner. Le portail contrefait utilisera des services basés sur ces technologies pour infecter la victime. Koobface utilise un lien vers une contrefaçon du portail Youtube utilisant un nom de domaine proche, afin de prêter volontairement à confusion. Cette astuce permet d'augmenter les

chances de réussite en se basant encore une fois sur la crédulité des personnes ciblées. Les liens envoyés par le ver sont ainsi du type :

```
http://www.YuoTube.com/[script_malveillant]
```

Ils dirigent l'utilisateur vers une page demandant à l'utilisateur d'installer une mise à jour de leur lecteur Flash pour pouvoir regarder la vidéo. Cette mise à jour n'en n'est bien sûr pas une puisqu'elle permet d'installer le premier composant nécessaire au fonctionnement de Koobface. Cet exécutable correspond au composant *downloader* de Koobface. Il se charge de télécharger différents composants permettant :

- la propagation *via* un réseau communautaire,
- la mise en place d'un serveur web permettant d'héberger le portail contrefait,
- le remplacement des serveur DNS de la machine par d'autres corrompus,
- l'installation ou le remplacement de l'anti-virus par un corrompu,
- la diffusion de publicité dans le trafic de l'utilisateur,
- de casser des CAPTCHA,
- la compromission de l'intégrité des recherches web de l'utilisateur.

Les réseaux utilisés par la victime sont identifiés grâce aux cookies stockés sur sa machine. Seuls les modules de propagation correspondants sont téléchargés et exécutés. Les cookies permettent également au ver de s'authentifier pour pouvoir utiliser les fonctionnalités de communication mises à disposition sur les portails web.

2.3 Des Vecteurs de Propagation Nombreux

Les méthodes de propagation que nous allons étudier maintenant utilisent des liens hypertextes vers des portails web contrefaits. Ces sites utilisent principalement des techniques de *phishing* pour abuser leur victime.

La messagerie électronique est un moyen de propagation éprouvé en matière de diffusion virale. La possibilité d'envoyer des messages formatés en HTML permet d'usurper la charte graphique d'un

portail communautaire. De plus, le protocole SMTP est très laxiste et permet à n'importe qui d'usurper n'importe quelle format d'adresse. Il est parfaitement envisageable d'envoyer un message à *victime@domain.tld* avec comme adresse d'expéditeur :

```
<FaceBook VIP Service> <vip_service@facebook.com>
```

La plupart des réseaux communautaires possèdent un système de messagerie interne permettant aux utilisateurs de dialoguer en privé. Il est alors possible d'envoyer des messages aux personnes faisant partie de son groupe d'amis ; que ces messages soient émis par une personne physique dûment autorisée ou par un *malware* cherchant à se propager. Le mur est un dispositif permettant à l'utilisateur de déposer un message à l'attention de l'ensemble de son cercle d'amis ; ces derniers peuvent également y écrire. Chacun de ces messages prend alors la forme d'un morceau de page web qui s'intègre au profil de l'utilisateur. Il est donc possible de *tagger*, c'est-à-dire d'écrire, sur le mur des personnes de son groupe d'amis ; que ces *tags* soit émis par une personne physique dûment autorisée ou par un logiciel malveillant cherchant à se propager.

Une autre possibilité offerte par ces API est de permettre aux utilisateurs de soumettre des applications, qui après un processus de validation seront acceptées ou non puis intégrées au portail. L'utilisateur pourra alors choisir parmi celles acceptées et ajouter tel ou tel composant à son profil. On remarque ainsi les problèmes que cela représente pour la communauté :

- Code non maîtrisé par le portail pensé à tort comme étant de confiance,
- Processus d'audit du code des applicatifs soumis inconnus.

2.4 Des Vecteurs d'Attaque Simples

Comme le prouve l'étude réalisée par Sophos, les techniques de *social engineering* n'ont pas à être particulièrement évoluées pour être efficaces. Le fait de duper sa victime est devenu courant dans la plupart des attaques :

- Reproduction de formulaire,
- Usurpation de charte graphique,
- Redirection des utilisateurs depuis des sites de confiance,

– Exécutable camouflé,
– etc.

Il existe de nombreux services sur l'Internet permettant de réduire la taille des adresses des liens que diffusent les internautes. Pour ce faire, on donne un lien que l'on estime trop long à un outil tel que tinyurl, et ce dernier nous donne en retour un lien plus compact de la forme *http ://tinyurl.com/yjnxsfu*. Ce lien est une redirection vers la page à l'adresse trop longue. Ce type de service est très prisé des utilisateurs de réseaux sociaux, notamment par ceux de Twitter où le nombre de caractères d'un message est par définition restreint. Tous les utilisateurs de Twitter sont donc habitués à cliquer sur ces liens hypertextes, qui ne donnent aucune indication sur la nature de la page ou du document cible. Des personnes mal intentionnées peuvent se servir de ceci pour attirer leurs victimes vers des pages au contenu malveillant. Il est par exemple possible d'annoncer sur Twitter la disponibilité d'une nouvelle version d'un logiciel apprécié, et d'en proposer le téléchargement directement *via* un lien hypertexte. Le lien proposé serait en réalité une redirection tinyurl vers l'exécutable d'un *malware*.

Comme sur tout système informatique, des vulnérabilités sont régulièrement trouvées sur les plates-formes communautaires. Par exemple sur le réseau social Facebook, certaines vulnérabilités XSS ont été identifiées. Le *cross-site scripting*, en abrégé XSS, est un type de faille de sécurité que l'on trouve typiquement dans les applications web qui peuvent être utilisées par un attaquant pour faire afficher aux pages web du code arbitrairement. Le principe consiste à injecter des données arbitraires dans une variable, par exemple en déposant un message dans un forum, ou en insérant des paramètres dans l'URL. Si ces données sont intégrées telles quelles dans la page web transmise au navigateur sans avoir été vérifiées, alors il existe une vulnérabilité : une personne malveillante peut s'en servir pour faire exécuter du code malveillant (Javascript le plus souvent) par le navigateur web qui se connectera à cette page. Voici un exemple de faille de type XSS qui a fonctionné sur le portail communautaire Facebook :

```
http://2.channel15.facebook.com/iframe/7/?pv=49&rev="> |
</script><title>Google</title></head></body><IFRAME \
src="http://www.google.com/" type="text/html" \
```

```
width="100%" height="100\%"></IFRAME>
```

Il est possible d'encoder cette URL douteuse pour aboutir à quelque chose de plus rassurant pour l'utilisateur car moins compréhensible :

```
http://2.channel15.facebook.com/iframe/7/?pv=49&rev= \
%22%3E%3C/script%3E%3Ctitle%3EGoogle%3C/title%3E%3C/ \
head%3E%3C/body%3E%3CIFRAME%20src%3D%22http%3A//www. \
google.com/%22%20type%3D%22text/html%22%20width%3D%22 \
100%25%22%20height%3D%22100%25%22%3E%3C/IFRAME%3E
```

Cette URL pourrait très bien être utilisée en conjonction avec une autre faille de type XSRF dans une attaque consistant par exemple à :

- Obtenir une liste d'amis sur un portail,
- Récupérer une adresse e-mail,
- Poster un message,
- etc.

Les attaques de type *cross-site request forgeries* (abrégées XSRF ou parfois CSRF) utilisent l'utilisateur comme déclencheur, celui-ci devient complice sans en être conscient. L'attaque étant actionnée par l'utilisateur, un grand nombre de systèmes d'authentification sont contournés. Le XSRF est une attaque instantanée. Elle ne repose pas sur l'exécution d'un script dans un navigateur. Son but est d'exécuter une action non désirée par le client sur un site où la victime possède un accès privilégié. Par exemple, un internaute participe à un forum de discussion sur lequel il est en conflit avec un modérateur. En guise de représailles, l'utilisateur décide de lui envoyer un message privé piégé exploitant une faille de type XSRF. La plupart de ces systèmes de messagerie intègrent un langage de type BBcode permettant aux utilisateurs d'insérer des images, des liens, des marques de formatage. Le message piégé contiendra par exemple le code :

```
[img]http://site\_victime/logout.php[/img]
```

qui une fois traduit en HTML par le moteur du site aura comme forme :

```
<img src='http://site_victime/logout.php' />
```

Les balises *img* représentent l'un des vecteurs d'attaque les plus répandus. Le navigateur ne fait aucune différence entre une requête HTTP GET vers une image ou vers une page. On voit ici quel impact pourrait avoir une requête particulièrement travaillée et envoyée à l'insu de la victime. Facebook a été vulnérable à ce type d'attaques. Koobface exploite depuis peu des vulnérabilités côté client pour infecter ses victimes. Il n'est plus nécessaire de forcer l'utilisateur à télécharger et à lancer un exécutable. L'infection devient complètement invisible. Il suffit que le navigateur de la victime ou l'un de ses composants ne soit pas à jour pour qu'il devienne facile d'exploiter une faille et installer une application malveillante. Les auteurs de Koobface ciblent bien entendu plusieurs vulnérabilités pour augmenter leurs chances de réussite. On peut citer notamment : VBS/Psyme.BM, Exploit.Pidief.EX, Exploit.Win32.IMG-WMF, etc. *Nota Bene* : cette technique semble avoir été abandonnée par les auteurs très rapidement après sa mise en service.

3 Applications Facebook Malicieuses

Les concepts du web 2.0 amènent les utilisateurs à participer activement à la vie de communauté et à y créer du contenu. En effet, les portails web deviennent collaboratifs et tout le monde est invité à rédiger, créer, noter ou commenter. Les réseaux sociaux vont encore plus loin en proposant à des développeurs tiers de créer leurs propres applications, afin d'apporter plus de fonctionnalités. Celles-ci seront intégrées ou non au portail après un processus de validation. Ces applications connaissent aujourd'hui un franc succès ; il en existent des dizaines de milliers regroupant plusieurs millions d'utilisateurs [4]. Facebook a mis en place un ensemble de mécanismes pour permettre aux développeurs de créer et de diffuser leurs applications. Comme tout environnement permettant la création d'applications tierces, Facebook est devenu vulnérable à certains contenus malveillants. Quelques applications malicieuses ont d'ores et déjà circulé sur Facebook, ce qui prouve les faiblesses des contrôles effectués.

3.1 Un Environnement Permissif

Facebook Platform est l'environnement qui a été mis en place pour permettre aux développeurs de créer leurs applications. Il est in-

contestablement simple à utiliser et extrêmement puissant. Les possibilités d'interaction avec les utilisateurs sont nombreuses, et se font par le biais d'une API riche et rapide à prendre en main [6]. Si ces possibilités incitent les développeurs à créer leurs applications, elles facilitent également le travail de personnes malveillantes désirant s'emparer des informations personnelles des utilisateurs. En effet, la nature même de Facebook amène ses membres à enregistrer sur leur profil un certain nombre d'informations personnels : nom, prénom, coordonnées, centres d'intérêts, etc. De plus, l'activité d'un utilisateur sur Facebook consiste principalement à parler de lui, c'est-à-dire à communiquer sur sa vie privée. Les applications ont donc, grâce aux API, accès à un nombre impressionnant de données personnelles. Il s'agit là d'un véritable trésor pour les spammeurs, et pour les personnes recherchant des données facilitant l'ingénierie sociale.

Il existe deux types d'applications Facebook : celles de type « iframe » et celles de type « FBML ». La première catégorie est dangereuse par nature ; elle permet aux développeurs d'intégrer directement dans un canevas un site distant (*cf.* Figure 1). Il est difficile de concevoir comment Facebook peut contrôler le comportement de ces applications. Peu importe le contenu, la page sera affichée à l'intérieur de l'interface Facebook. La seconde catégorie n'est pas intégrée directement dans le canvas. Un « pré-traitement » est effectué par la plateforme Facebook qui récupère depuis le serveur distant un ensemble de données au format Facebook Markup Langage (FBML). Ce langage spécifique à Facebook permet la mise en forme et l'appel direct aux fonctions de l'API. Dans tous les cas, les applications tierces sont situées sur un site distant, échappant ainsi au contrôle de Facebook. Les appels aux API sont réalisés *via* une bibliothèque que les développeurs importent et déploient sur leur serveur.

Les mécanismes qui ont été mis en place par Facebook pour permettre l'intégration d'applications tierces sont donc extrêmement permissifs. N'importe quelle page web peut-être intégrée dans l'interface de l'utilisateur. Ainsi, Facebook n'a aucun contrôle sur le contenu des applications, qui sont pourtant diffusées à tous les utilisateurs du réseau. De la même manière, les applications étant situées sur un serveur distant inaccessible aux équipes Facebook, ces dernières ne peuvent suivre le cycle de vie des programmes. Les seuls contrôles pouvant éventuellement être réalisés seraient d'analyser l'utilisation

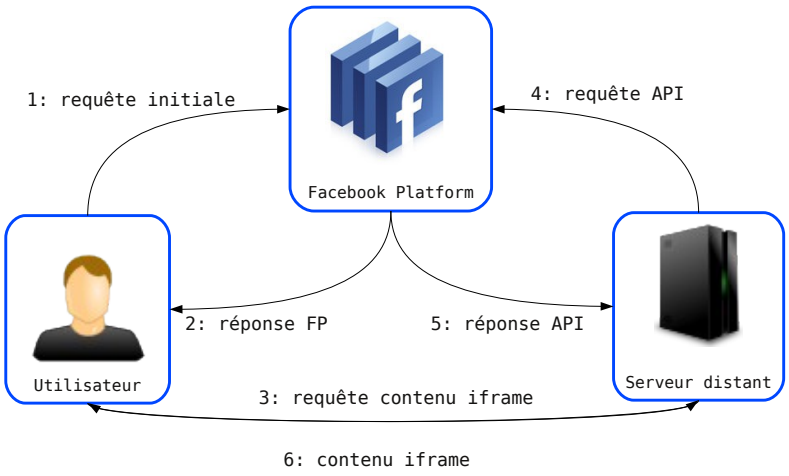

Figure 1. Dans le cas d'une application iframe, l'utilisateur est connecté directement à un serveur distant, sans qu'il n'ait quitté l'environnement Facebook.

des méthodes des API, afin de détecter d'éventuels comportements suspects. Malheureusement ce type d'analyse ne donne que peu de résultat (problème des faux positifs par exemple), et au vue de la quantité d'applications cette tâche semble être impossible à réaliser.

3.2 Des Fonctionnalités Indiscrètes

Les appels aux fonctions des API sont la base de toute application Facebook, car ce sont elles qui permettent d'interagir avec les données des utilisateurs. Ainsi, dès qu'un utilisateur désire installer une application sur son profil, un message l'informe que l'application aura accès à ses données personnelles. L'acceptation de cet accès est nécessaire à l'installation de toute application tierce. A chaque installation, l'utilisateur doit donc valider ce message : *« Le fait d'attribuer un accès à l'application lui permettra d'accéder aux informations de votre profil, à vos photos, aux informations sur vos amis et à tout autre contenu nécessaire à son fonctionnement. »*. Un effet de bord de cette validation systématique est que les utilisateurs n'y prêtent plus attention. En effet, il s'agit d'un message qui ne sera lu qu'une seule fois, et au fil des installations sera oublié, voire confondu avec une validation de l'installation. Pourtant, l'utilisateur permet à une application non contrôlée de connaître toutes ses données personnelles, ainsi que celles de ses amis, même s'ils n'ont pas installé l'application ni accepté l'accès à leurs données. Ceci permet donc à un développeur tiers de constituer une base de données très complète sur un nombre important de personnes, pour peu que son application rencontre du succès. Par exemple, il peut sans contraintes reconstituer les relations sociales entre les utilisateurs, et ainsi découvrir des relations que les membres ne connaissent pas forcément eux-mêmes. De manière générale, quasiment toutes les informations sont accessibles aux applications ; ceci s'apparente à un accès en lecture seule.

Il existe également ce que l'on appelle des « possibilités étendues », permettant aux développeurs d'obtenir un accès en écriture sur le profil des utilisateurs ayant installé l'application. Pour un développeur malveillant, ceci est plus contraignant à mettre en place, car il doit faire accepter à l'utilisateur accès par accès les droits supplémentaires de son application. Le jeu en vaut cependant la chan-

delle, car il peut ainsi ajouter des photographies au profil, publier sur le mur, rédiger des commentaires et créer des pages d'évènements. Il est également possible, de manière similaire, d'envoyer des e-mails aux utilisateurs, de lire leur messagerie personnelle Facebook, de diffuser des liens hypertextes sous l'identité de l'utilisateur, et d'accéder à toutes les données de l'utilisateur même s'il est déconnecté. Si les possibilités de base sont inquiétantes, les possibilités étendues sont proprement affolantes : une application peut prendre le contrôle total d'un compte Facebook. La validation accès par accès obligatoire limite le champ d'action de développeurs malveillants, mais un problème classique leur facilite la tâche : à force de valider constamment des accès aux applications, la plupart des utilisateurs ne sont plus méfiants et acceptent systématiquement toutes les demandes. Ce problème est agravé du fait que les membres de Facebook accordent généralement une confiance aveugle à leur réseau social favori.

3.3 Des Intégrations Portant à Confusion

Les applications développées par les tiers prennent différentes formes. Une fois installé, un programme peut être affiché de plusieurs manières différentes au sein de l'interface Facebook de l'utilisateur. Ces formes sont tellement nombreuses qu'il devient difficile de distinguer une application tierce d'une fonctionnalité officielle.

Une application peut par exemple prendre la forme d'une boîte affichée sur le profil de l'utilisateur, c'est-à-dire l'espace principal associé à une personne. Située à gauche, cette boîte est strictement identique aux éléments authentiques comme la liste d'amis ou les informations de la personne. La page de profil d'une personne contient de même un ensemble d'onglets qui permettent d'accéder aux différentes données de l'utilisateur, typiquement ses informations personnelles, son mur et ses photos.

Une application tierce peut également prendre la forme de l'un de ses onglets. L'onglet « Infos » du profil d'une personne permet d'afficher les informations personnelles de l'utilisateur, comme ses coordonnées et son parcours professionnel. Une application tierce peut ajouter un ensemble de données à cette page. Lorsque l'utilisateur désire publier du contenu sur son mur ou sur celui de ses amis, des outils de publication lui sont proposés. Ces outils permet-

tent de diffuser du texte simple, des images, des vidéos ou des liens hypertextes. Une application tierce peut venir ajouter un outil de publication, pour permettre à l'utilisateur de publier des données générées par le programme.

Les applications Facebook développées par des tiers ont la possibilité de se fondre dans l'environnement officiel. Dès lors, il peut devenir très compliqué pour un utilisateur non averti de distinguer ce qui est authentique de ce qui ne l'est pas. Ainsi, les utilisateurs peuvent utiliser sans le savoir des outils sur lesquels les équipes Facebook n'ont aucun contrôle, et pourtant leur faire confiance. Si ces possibilités d'intégration permettent aux applications « saines » d'améliorer l'expérience de l'utilisateur en fournissant des interfaces unifiées, elles permettent également aux personnes malveillantes de créer des *malwares* se confondant avec les outils officiels. Ceci représente un grave danger, car les évolutions sont nombreuses et les utilisateurs ne peuvent savoir si un nouvel outil présent dans leur interface est développé par Facebook, ou par une personne malveillante.

3.4 Une Diffusion Virale

Lorsqu'une application a été développée par un tiers, Facebook offre différents moyens de diffusion, pour permettre aux utilisateurs de partager les applications qu'ils aiment, et aux développeurs de faire connaître leur production.

Le répertoire des applications est l'espace principal dédié aux différentes applications disponibles. Il s'agit du point central à partir duquel les utilisateurs peuvent rechercher des applications par mot-clé, par thème ou par popularité. Elles sont toutes disponibles *via* cette interface. Chaque application est présentée par un nom, une image, une description et une cote de popularité. Mis à part la popularité, tous les autres paramètres sont édités par les développeurs. Les utilisateurs peuvent installer directement une application sur leur profil à partir de cet espace. Pour cela, un utilisateur sélectionne une application à partir du répertoire ; il est alors dirigé vers la page d'accueil de l'application, c'est-à-dire l'espace où est détaillé le fonctionnement, les membres, etc. Le contenu de la page d'une application est maîtrisé par le développeur de l'application en question. Il défini donc librement l'image, la description et le nom du

programme. Les utilisateurs peuvent également participer au contenu de cette page, en lui attribuant une notation ou en écrivant un commentaire. Un avertissement discret prévient les utilisateurs lorsqu'il s'agit d'une application tierce : *« Cette application n'a pas été développée par Facebook »*. Aucune autre indication n'explicite les risques encourus.

Un utilisateur qui apprécie une application peut inviter ses amis à l'utiliser également. En général, les applications proposent à leurs utilisateurs d'inviter leurs amis directement après l'installation. Les amis de l'utilisateur reçoivent alors une

notification, qui leur permet d'installer l'application immédiatement. Les applications peuvent également prendre différentes formes sur le profil d'un utilisateur. Ainsi, ses amis peuvent prendre connaissance de l'application en parcourant son profil. Plus un programme tiers utilise les fonctionnalités d'intégration de Facebook, plus il sera présent sur un profil. Cette présence sur profil se rapproche du bouche-à-oreille et offre de cette manière un moyen de diffusion très efficace. La plupart des applications publient directement sur le mur de leurs utilisateurs des informations sur leur utilisation. Par exemple, dans le cas d'un jeu, l'application diffuse sur le mur le score de son utilisateur. En apparaissant sur le mur d'une personne, cette notification sera diffusée à l'ensemble de son cercle d'amis sur leur page d'accueil, qui résume les actualités.

Les moyens de diffusion d'une application sont simples à mettre en œuvre et extrêmement efficaces. Toutes celles ayant du succès se diffusent ainsi de manière très rapide. Ces techniques de diffusion constituent cependant autant de moyen de propagation pour les *malwares*. Camouflé en application saine, un programme malveillant dispose de multiples moyens pour se propager simplement et efficacement.

3.5 Des Applications Malveillantes Actives

Certaines applications de Facebook sont conçues pour être malveillantes. La raison de leur création reste le plus souvent monétaire. C'est pourquoi nous pouvons nommer ces applications *malwares actifs*, à l'inverse des *malwares passifs* dont l'utilisation initiale « saine » peut être détournée pour obtenir un comportement malveillant.

Photo Stalker est un *malware* actif présent sur Facebook. Cette application est considérée comme malicieuse car elle permet à ses utilisateurs d'accéder aux photographies de l'ensemble des utilisateurs du portail, y compris de ceux qui ne font pas partie de leur cercle d'amis. Le danger de cette application est réel, car il rend accessible à n'importe qui des photos qui peuvent avoir un caractère strictement personnel, simplement à partir d'un nom. Cette application ne contourne aucun mécanisme de sécurité, mais utilise simplement une propriété d'importation des photographies sur le réseau. En effet, par défaut, les image chargées par les utilisateurs sont marquées comme étant publiques, c'est-à-dire que n'importe quel membre de Facebook peut y accéder, moyennant la connaissance de leur existence. Photo Stalker se charge de trouver ces photos publiques, et de les rendre accessibles à tous. Le but de cette application est en réalité de dénoncer ce problème de confidentialité, en montrant comment il est possible de l'exploiter à grande échelle. Les équipes Facebook ont réagi en juillet 2009 en modifiant le comportement par défaut à l'importation de photos, qui les rend désormais inaccessibles a tous, à moins que le propriétaire des images ne change explicitement ces paramètres.

Des chercheurs de l'Institute of Computer Science (ICS) ont démontré comment, à partir d'un système de réseau social comme Facebook, il était possible de créer un « réseau anti-social » [5]. Selon leur rapport publié en juin 2008, les réseaux anti-sociaux sont des systèmes distribués basés sur des portails de réseaux sociaux, qui peuvent être exploités par des attaquants, et dirigés pour former des attaques par le réseau. Afin de démontrer comment constituer un réseau anti-social, les chercheurs de l'ICS ont développé une application Facebook : *Photo Of The Day*. Le rôle de cette application est d'afficher, chaque jour, une image en provenance de l'organisme National Geographic sur le profil de ses utilisateurs. Ce programme est une application de type *iframe*, c'est-à-dire qu'elle intègre directement dans l'environnement de son utilisateur un contenu situé sur un serveur distant. Un comportement caché a également été ajouté à l'application. Ainsi, à chaque fois qu'un utilisateur de l'application désire afficher l'image du jour, il effectue également à son insu une requête HTTP vers un serveur victime. Il s'agit d'une attaque par déni de service distribué, ou *DDOS* (Distributed Denial Of Ser-

vice). Concrètement, l'application Photo Of The Day intègre quatre *iframes* cachés, qui font chacune référence à une image hébergée sur le serveur victime. Chaque iframe crée de cette manière une requête HTTP GET demandant au serveur attaqué de renvoyer X Ko de données. Les éléments étant cachés, l'utilisateur ne peut apercevoir la manipulation. Voici le code d'un iframe malicieux :

```
<iframe name="1" style="border: 0px none #ffffff;
  width: 0px; height: 0px;"
  src="http://victim-host/image1.jpg?
  fb_sig_in_iframe=1&amp;
  fb_sig_time=1202207816.5644&amp;
  fb_sig_added=1&amp;
  fb_sig_user=724370938&amp;
  fb_sig_profile_update_time=1199641675&amp;
  fb_sig_session_key=520dabc760f374248b&amp;
  fb_sig_expires=0&amp;
  fb_sig_api_key=488b6da516f28bab8a5ecc558b484cd1&amp;
  fb_sig=a45628e9ad73c1212aab31eed9db500a \fg{}
</iframe>
```

La déclaration *style="border : 0px none #ffffff ; width : 0px ; height : 0px ;"* permet de dissimuler l'affichage de l'iframe, et donc de l'image téléchargée sur le serveur victime. Les autres déclarations permettent à l'application d'utiliser les services Facebook pour charger l'image. Cette attaque ne peut être efficace que si de nombreuses requêtes sont dirigées en même temps vers la victime. En d'autres termes, plus il y a d'utilisateurs de cette application, plus la probabilité de créer un déni de service sur le serveur victime est élevé. Nous avons vu que Facebook propose de nombreux moyens de propagation permettant d'augmenter le nombre d'utilisateurs d'une application. Facebook étant un réseau social, on constate que les utilisateurs sont souvent connectés aux mêmes horaires, afin de communiquer de manière instantanée, ou pour suivre l'actualité de leurs cercle d'amis. En utilisant les moyens de diffusion fournis et en exploitant les propriétés sociales de leur mécanisme, les chercheurs sont parvenus à obtenir rapidement un nombre de requêtes important dans un court laps de temps. En analysant le trafic généré sur le serveur victime (en réalité un serveur de test en leur possession), ils ont pu établir que si les applications les plus populaires de Facebook, bénéficiant chacune de plus de 2 millions d'utilisateurs actifs, intégraient des mécanismes d'attaque similaires, le serveur victime aurait un trafic non sollicité de 23 Mb/s, et recevrait sur une période d'un jour environ 248 Go de

données non désirées. Les chercheurs sont donc arrivés à la conclusion que ce type d'attaque pourrait être extrêmement efficace, pour peu qu'elle soit mise en œuvre sur une application rassemblant un grand nombre d'utilisateurs. A partir de ces résultats, les chercheurs ont mis en avant d'autres types d'attaques possibles utilisant des mécanismes similaires :

- Scan d'hôtes : à l'aide d'un code Javascript, un attaquant peut déterminer quels ports sont ouvert sur une machine. Puisque les navigateurs ne restreignent que quelques ports de destination, un attaquant peut envoyer à sa victime des requêtes de connexion HTTP sur un port choisi et en se basant sur le temps de réponse, qui peut être mesuré avec Javascript, il peut connaître l'état du du port : actif ou non.
- Attaque basée sur les cookies : de la même manière que les vers XSS, une application malicieuse peut écraser les mécanismes d'authentification qui sont basés sur les cookies. Les sites mal concus qui supportent l'identification en utilisant des cookies sont vulnérables à ce type d'attaque.
- Propagation de *malware* : un utilisateur peut participer à son insu à la propagation d'un logiciel malveillant. Si un serveur peut être exploité par une attaque *via* une URL, alors une application Facebook peut servir de moteur d'exploitation. Chaque utilisateur qui interagirait avec l'application en question propagerait le vecteur d'attaque.

Stream est le nom d'une application FaceBook utilisant des techniques de *phishing* pour tromper les utilisateurs et les forcer à installer l'application. La technique consiste à utiliser des vecteurs de propagation classiques (e-mails, mur, message privé, etc.) pour diffuser des messages contenant un lien HTML. Le lien en question pointe vers un nom de domaine fucabook.com proche de l'original permettant de tromper les moins vigilants. La page chargée ressemble trait pour trait au formulaire de connexion de Facebook. Après avoir entré son couple d'identifiants une première fois pour installer l'application, la victime se voit demander une seconde fois ces même informations *to use the full functionality of XXX*. Il s'agit en fait de donner l'autorisation d'accès aux données personnelles à l'application en mode hors-ligne (lorsque que l'utilisateur n'est pas connecté). Une fois l'application installée, elle va utiliser une photo du cercle

d'amis de la victime pour la prévenir que quelqu'un lui a envoyé un message. Elle démarre ensuite une phase de *spamming* pendant laquelle elle envoie aux amis de la victime le message contenant le lien HTML pointant vers le formulaire de connexion contrefait. Une chose intéressante à noter : l'icône de cette application ressemble étrangement à celles « officielles » utilisées sur le portail Facebook.

3.6 Des Applications Malveillantes Passives

Il existe également des *malwares* passifs ; c'est-à-dire qui ne sont pas malicieux, mais que les utilisateurs malveillants peuvent détourner pour en modifier le comportement.

C'est le cas de l'application Mood présente sur Facebook qui propose à ses utilisateurs de publier sur leur mur un smiley décrivant leur humeur du moment. Le choix de smiley est très vaste et permet de représenter toutes les situations. Une vulnérabilité de cette application disposant de plus de 150 000 utilisateurs actifs permet à une personne de diffuser le smiley qu'il désire sur le mur de n'importe quel autre utilisateur de l'application, qu'il soit dans son cercle d'ami ou non. En effet, à l'aide d'un outil de débogage dynamique type Firebug pour Firefox, il est possible de modifier les attributs de la requête envoyée par l'application pour publier le smiley. En modifiant la valeur de l'attribut *fb_sig_user* par l'identifiant d'un autre utilisateur, il est possible de faire afficher le smiley sur la page de cette autre personne. Cette vulnérabilité, qui a été rapidement corrigée par les développeurs de l'application, ne remet certes pas en cause la sécurité de Facebook. En revanche, elle permet d'imaginer quelles sont les attaques possibles sur des applications tierces, qui peuvent contenir elles aussi des informations privées sur les utilisateurs. De plus, pouvoir modifier aussi simplement les données du mur d'une personne est tout à fait inquiétant.

L'application ObserverFacebook permet à ses utilisateurs d'interagir avec les articles publiés sur le site Internet du journal américain The Charlotte Observer. Pour l'utiliser, les lecteurs doivent renseigner leurs noms, prénoms et adresses électroniques. Ils peuvent ensuite proposer des histoires et gagner des points popularité. Cette application s'est révélée vulnérable à des attaques de type injection SQL en novembre 2009. En effet, une de leur page inter-

prête directement un des paramètres GET de l'URL pour créer ses requêtes SQL, afin d'accéder aux informations demandées par l'utilisateur.Voici l'URL d'une requête normale :

```
http://apps.facebook.com/observerfacebook/ \
?p=challenges&id=42
```

En observant cette URL, on devine que le code situé sur le serveur distant de l'application effectue des opérations similaires à celle-ci :

```
identifiant = parametre <id> de l'URL
requete = "SELECT ? FROM ? WHERE id=" + identifiant
executer requ\^{e}te
```

Sans contrôle particulier, il est possible de modifier le comportement de la requête en injectant un morceau de requête SQL dans l'identifiant. Ce manque de contrôle couplé à un nom de table contenant les utilisateurs aisé à deviner, l'URL suivante permet d'obtenir l'ensemble des informations des utilisateurs enregistrés :

```
http://apps.facebook.com/observerfacebook/?p=challenges \
&id=-1+AND+1=2+UNION+SELECT+1,group_concat%28name,0x3a, \
email%29,3,4,5,6,7,8,9,10,11,12,13,14,15,16,17+from+-User
```

La valeur passée pour l'identifiant ajoute en fait une deuxième requête SQL à l'aide du mot clé UNION. Celle ci sera exécutée en même temps que la première, et permet d'interroger la table *User* afin d'en extraire toutes les données. Les équipes Facebook ont été alertées par cette vulnérabilité, et l'application a été rendue inaccessible aux utilisateurs jusqu'à ce qu'elle soit corrigée.

Dans le but d'estimer les possibilités de détournement d'applications Facebook, nous avons voulu tester sur une application populaire prise au hasard des techniques de piratages simples et communes. L'application Do you really know me ? permet de construire ses sondages et de les proposer sur son profil pour que son cercle d'amis y réponde. Un examen très superficiel des fonctionnalités proposées nous a permis de mettre rapidement en évidence une faille applicative de type XSS. Un formulaire permet de saisir les informations et les questions du sondage. Malheureusement le champ de texte permettant d'enregistrer le nom de la question ne filtre pas les balises de type *iframe*. Il est donc très facile de faire exécuter du code Javascript aux utilisateurs venant naïvement répondre au

sondage. De la même manière, le champ question permet d'insérer des balises HTML de type *img*, ce qui amène à une vulnérabilité de type XSRF. Il est tout à fait possible insérer le texte suivant en guise de question :

```
question <img src='[EVIL_SCRIPT_URL]' style='display: none;'/>
```

Ainsi, chaque utilisateur visitant le sondage malveillant effectura sans le savoir une requête HTTP en GET vers [EVIL SCRIPT URL]. A partir de ceci, une autre attaque consiste à récupérer les informations de l'internaute visitant la page :

```
question <img src='http://host/script.php' style='display: none
    ;'/>
```

Le script *http ://host/script.php* peut contenir un code permettant d'enregistrer les informations sur une machine maitrisée par l'attaquant :

```
<?php
$log_file="./test.log";
$info="User agent : $_SERVER[HTTP_USER_AGENT]\n";
$info.="Host :  $_SERVER[REMOTE_HOST] \
($_SERVER[REMOTE_ADDR])\n";
$info.="Referrer : $_SERVER[HTTP_REFERER]\n";
$info.="Query string : $_SERVER[QUERY_STRING]\n";
$info.="Date : ".date()."\n\n";
$file=fopen($log_file,"a");
fputs($file,$info);
fclose($file);
?>
```

Rien n'empêche l'URL de comporter des paramètres, et un scénario d'attaque consistant à récupérer des informations *via* un code Javascript inséré par XSS pour les récupérer sur un serveur distant en utilisant une faille de type XSRF est parfaitement viable. On comprend à travers ces exemples et au vu du nombre d'applications déployées que les failles de type XSS et XSRF facilement identifiables et exploitables représentent un réel danger.

3.7 Conclusion

Au vu du nombre impressionnant d'applications tierces disponibles sur Facebook, il est légitime d'avoir des doutes sur les contrôles réalisés pendant le processus de validation avant intégration. Il apparaît désormais clairement qu'ils sont insuffisants. On peut également

se demander si le comportement et le code de ces applications est réellement analysé, et quelle assurance peut-on avoir quand le code en question est hébergé sur un serveur non maitrisé par Facebook. Est-il identique au moment de sa validation et lorsqu'il est exécuté plusieurs mois après dans un navigateur ?

4 Diffusion d'une Application Sociale sur Facebook

4.1 Introduction

Deux types d'entités peuvent être intéressées par la diffusion d'applications sur les réseaux sociaux : les entreprises dans un but publicitaire, et les personnes malveillantes. Nous allons donc dans cette partie étudier comment concevoir une application de manière à faciliter sa propagation au plus grand nombre, et quels types d'informations peuvent être récoltées. Afin de prendre en compte tous les aspects de ce sujet, une application Facebook récoltant les informations de ses utilisateurs a été développée puis diffusée. Nous allons ainsi mettre en évidence comment utiliser les fonctionnalités offertes par l'API pour propager efficacement l'application. Des comptes fictifs ont ensuite été créés, dont le but est d'attirer le plus de contacts possible ; nous étudierons quelles techniques permettent d'amener les utilisateurs à accepter les requêtes d'ajouts aux listes d'amis. Enfin, nous avons diffusé l'application à partir des comptes fictifs pour mettre en avant comment diffuser le mieux possible une application. Toutes les données personnelles récupérées sur les utilisateurs de Facebook dans le cadre de notre étude ont été anonymisées dans nos bases de données, et ont été supprimées au terme de nos travaux.

4.2 Définir une Stratégie de Diffusion

Définir préalablement une stratégie de diffusion est primordial pour assurer une ample propagation de l'application. Pour ce faire, nous avons défini plusieurs étapes qui ont pour but d'inciter les utilisateurs du réseau social à installer l'application.

Que ce soit dans un but publicitaire ou dans un but malveillant, le ciblage des utilisateurs potentiels de l'application est primordial. En

effet, des fonctionnalités en décalage avec les attentes des utilisateurs seraient fatales pour la propagation du programme sur le réseau. Sur le réseau social Facebook, la tranche d'âge des 15-25 ans est manifestement la plus présente. De plus, cette génération est à l'aise avec ces nouvelles plateformes et particulièrement encline à utiliser et à partager les contenus qui sont mis à sa disposition. C'est donc tout naturellement que nous choisirons cette part des utilisateurs comme cibles de notre application.

La première étape de notre stratégie de diffusion sera la création de comptes fictifs, qui sont un excellent moyen de démarrer la propagation d'une application sociale [7]. Dans le cadre d'une entreprise souhaitant diffuser une application sociale à but publicitaire, cette méthode est bien sûr déconseillée pour l'image de marque, mais elle pourra par exemple les remplacer par les comptes de ses employés. En revanche, il s'agit d'un outil à nul autre pareil pour les personnes malveillantes souhaitant faire croire que leur application est populaire. Il est donc nécessaire de correctement préparer ces comptes fictifs, notamment afin qu'ils aient le plus d'amis réels possibles (*cf.* Figure 2).

La création d'un compte sur Facebook est extrêmement rapide : quelques champs doivent être renseignés, notamment un nom, une adresse électronique, un mot de passe, et un âge. Quelques contraintes sont imposées par la plateforme, notamment l'utilisation d'un nom crédible (sans caractères spéciaux ni chiffres), un âge minimum (13 ans) et un CAPTCHA à renseigner. Puisque le but de ces comptes fictifs est d'attirer le plus d'amis possibles, un nom et un âge crédibles doivent de toutes manières être entrés. Bien sûr, une adresse électronique ne doit correspondre qu'à un unique compte ; une adresse électronique différente doit donc être créée pour chaque compte fictif, ce qui se fait facilement si l'on dispose d'un serveur de messagerie, ou en utilisant des services gratuits tels que Hotmail ou Yahoo !. Cette adresse est nécessaire pour valider la création de compte sur Facebook, de plus elle ne doit pas sembler suspecte pour pouvoir être affichée dans les informations du profil fictif. *Prenom.Nom@domain.tld* est par exemple un format d'adresse tout à fait plausible. L'étape suivante du processus d'inscription de Facebook consiste à demander le parcours scolaire et professionnel de l'utilisateur. Ceci permet ensuite à la plateforme de proposer un cer-

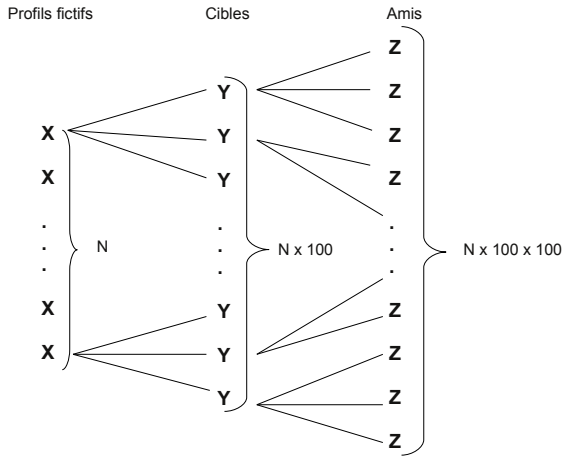

Figure 2. En comptant une moyenne de 100 amis par profil d'utilisateur du réseau social, et en partant de N comptes fictifs, $N * 10000$ personnes peuvent être atteintes dès le deuxième degré de diffusion.

tains nombre de personnes, 51 exactement, que l'utilisateur a probablement côtoyé, car les établissements / entreprises et les promotions correspondent. Il s'agit de l'unique moment où l'utilisateur peut inviter des personnes sans avoir à saisir de CAPTCHA. Par la suite en effet, toute demande nécessitera cette fastidieuse tâche, à moins d'entrer un numéro de téléphone portable qui sera validé par SMS, ce qui est difficilement concevable de fournir dans le cadre de la création d'une multitude de comptes fictifs. Cette opportunité doit donc être saisie, d'autant plus que les personnes visées par les demandes verront quelqu'un qu'ils ont sans doute rencontré à un moment de leur vie, et seront ainsi plus enclines à accepter l'ajout à la liste d'amis du compte fictif. De plus, une astuce permet d'augmenter cette liste de 51 personnes à 360, limite à partir de laquelle Facebook bloque la fonctionnalité de demande d'ajout temporairement, simplement en validant l'étape puis en demandant le retour à l'étape précédente. Enfin, Facebook propose de télécharger une photo de profil. N'importe quelle image est possible, mais il semble qu'une

photo représentant vraisemblablement le propriétaire du compte soit plus efficace pour augmenter le nombre d'amis du profil.

La deuxième étape consistera à envoyer un message aux comptes cibles. Par exemple, l'application pourra envoyer automatiquement un message sur le mur de l'utilisateur lorsqu'elle sera installée. Ainsi, si l'application sera installée sur 20 comptes fictifs, et si chaque installation affiche un message sur le mur de l'utilisateur, alors un message sera affiché dans les fils d'actualités de 2000 cibles ;

il s'agit du premier degré de diffusion (*cf.* Figure 3). La suite de notre stratégie consistera à réitérer cette étape au premier degré, en se basant toujours sur l'envoi de messages sur le mur. Ces différentes itérations peuvent être considérées comme autant de rappels. En parallèle, une page Facebook sera créée pour l'application, et chaque compte fictif en deviendra fan. De plus, chaque profil fictif ajoutera un avis positif à l'application, et l'ajoutera à ses favoris, afin de forger la réputation de l'application sociale.

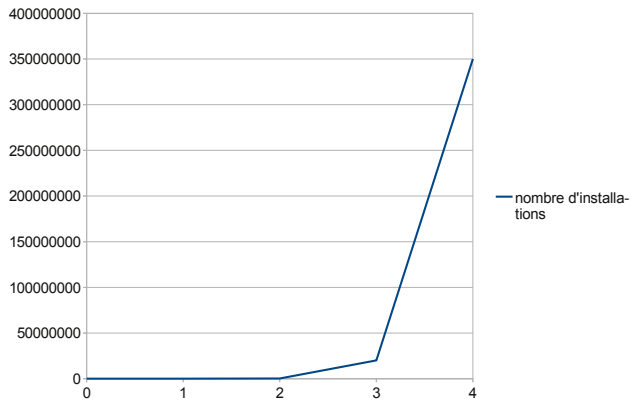

Figure 3. Dans le cas idéal, et bien évidemment très loin de la réalité, où chaque personne recevant un message dans ses actualités installe l'application, il est possible d'atteindre tous les utilisateurs de Facebook, soit 350 millions de personnes [8], dès le 4ème degré de diffusion et avec une base de seulement 20 comptes fictifs.

4.3 Développer une Application

Cette partie décrit certains choix de développement de

l'application sociale, notamment afin de permettre la mise en œuvre de la stratégie de diffusion préalablement établie.

Deux types de fonctionnalités sont susceptibles d'intéresser notre cible : les fonctionnalités amusantes et les fonctionnalités utiles. Nous appelons fonctionnalités utiles celles qui apportent quelque chose que le réseau social ne propose pas nativement, et qui améliorent l'expérience d'utilisation de la plateforme. Nous nous sommes focalisés sur cette dernière catégorie. Partant du constat que Facebook n'informe pas l'utilisateur lorsque l'un de ses contacts l'a supprimé de sa liste d'amis, nous avons décidé de créer une application apportant cette fonctionnalité. Ainsi, l'application sociale affiche une mosaïque composée des avatars des amis de l'utilisateur, ainsi qu'une liste de ses contacts qui l'ont supprimé de leur liste. L'utilisateur remarque qu'une personne l'a supprimé de sa liste si une croix rouge est affichée par dessus son avatar.

Un des problèmes les plus importants que l'on rencontre lorsque l'on souhaite développer une application sociale destinée à être largement diffusée est paradoxalement le dynamisme des évolutions de la plateforme. Par exemple lors de notre développement, nous avons pu constater que Facebook a modifié plusieurs fois sa politique en matière de fonctionnalités permettant aux applications de se diffuser. Notamment, nous avons pu noter que :

- La fonctionnalité d'invitations d'amis à utiliser une application a été limitée à 8 personnes,
- Les applications ne peuvent plus envoyer de messages directement dans la zone de notification de l'utilisateur,
- Lorsqu'une personne demande à quelqu'un leur mise en relation, des suggestions de connaissances ne sont plus affichées ; c'est la personne qui reçoit l'invitation qui a la possibilité de proposer des connaissances à la personne demandeuse.

Ces changements ainsi que les nombreux autres déjà en place ou étant prévus gênent la mise en place d'une stratégie de diffusion, mais montrent la volonté de Facebook de régulariser la gestion des applications, et donc d'améliorer la confidentialité des données per-

sonnelles des utilisateurs, tout du moins vis-à-vis des développeurs d'applications sociales.

Pour éviter à l'utilisateur de se connecter à l'application à chaque fois qu'il désirer vérifier l'état de sa liste d'amis, et surtout pour informer ses amis qu'il utilise l'application, un message est écrit sur son mur lorsqu'une personne l'a supprimé de sa liste. Cet envoi de message nous permettra de mettre en œuvre les rappels de notre stratégie de diffusion. Ainsi, ce message apparaît dans le fil d'actualités de la page d'accueil de chacun de ses amis. Ce type de communication est le moyen de propagation principal que nous avons choisi. En effet, ces messages qui apparaissent dans le fil d'actualités bénéficient d'une forte visibilité, sur tous les amis de l'utilisateur, et, contrairement à de simples notifications, inspirent confiance car il semblent venir de l'utilisateur lui-même. Un message de ce type est également écrit sur le mur de l'utilisateur lorsqu'il vient d'installer l'application. Enfin, un message électronique est envoyé sur la boîte personnelle de l'utilisateur *via* l'API Facebook afin de l'informer lorsqu'un de ses contacts l'a supprimé.

4.4 Des Résultats Encourageants

Dans le cadre de notre étude, 21 comptes fictifs ont été créés, en utilisant diverses techniques pour amener les personnes visées à accepter nos ajouts à la liste d'amis. Nous avons pu constater que 38,6% des 5043 personnes visées ont accepté nos demandes, c'est-à-dire 1948 personnes au total. Il est intéressant d'observer les résultats obtenus selon le type de compte fictif créé (*cf.* Table 1). Toutes les catégories n'ont pas un nombre équivalent de profils fictifs ; la moyenne des pourcentage obtenus est donc différente de la moyenne globale.

Table 1. Taux d'acceptation selon le type de profil fictif.

Type de profil	*Avatar*	*Orientation avatar*	*Acceptations*
Réaliste	Crédible	Aguichant	51 %
Réaliste	Crédible	Neutre	42 %
Réaliste	Fantaisiste	Neutre	17 %
Fantaisiste	Fantaisiste	Neutre	14 %

On remarque ainsi que les utilisateurs du réseau social acceptent plus facilement les demandes provenant de profils réalistes et crédibles. Ceci tient sans doute également au fait que les profils fictifs ciblent des personnes ayant un parcours scolaire et professionnel bien précis, en se faisant passer pour quelqu'un ayant suivi ce même parcours. Les cibles sont donc mises en confiance en voyant quelqu'un qui semble être réel et qu'elles ont probablement côtoyé. Créer des profils fictifs fantaisistes, en se faisant passer pour des personnages de dessins animés par exemple, ne semble pas être payant. En revanche, utiliser un avatar crédible mais représentant une personne « bien constituée » permet de rapporter quelques acceptations supplémentaires, bien qu'il ne s'agisse manifestement pas du critère principal.

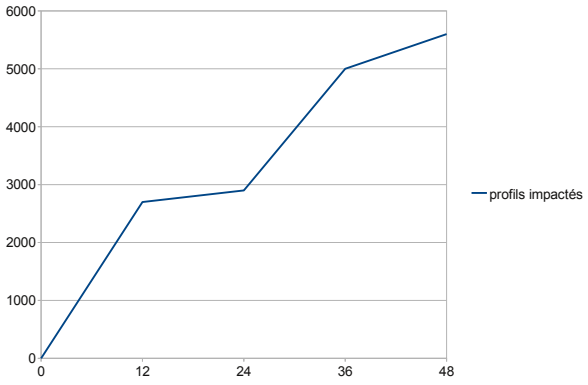

Figure 4. L'installation de l'application sur les profils fictifs a été éffectuée à $t=0h$. À $t=24h$, un message été envoyé sur les fils d'actualités des amis des comptes fictifs.

Pour suivre l'évolution de la diffusion de l'application sociale, nous nous basons non pas sur le nombre de profils qui ont installé l'application, mais sur ce qui intéresse vraiment une entreprise ou une personne malveillante : le nombre de profils impactés par la récolte de données personnelles (*cf.* Figure 4). On remarque immédiatement que sans intervention de notre part, l'évolution de la diffusion stagne. Propager une application sociale est donc une tâche qui doit s'éten-

dre dans le temps et nécessite un certain suivi. Les étapes de rappel doivent ainsi être itérées régulièrement, de manière à assurer le maximum d'installation de la part des cibles ; la suite de la diffusion se fera ainsi naturellement.

L'application sociale nous a permis de récolter automatiquement les informations personnelles de 5618 profils du réseau social, à partir de 21 comptes fictifs. Il est manifeste que les personnes impactées n'ont pas suffisamment pris garde à protéger leurs données. La Table 2 récapitule les données que nous avons pu récolter.

Table 2. Taux d'informations accessibles lors de la récolte.

Type d'informations	*Récolte*
Date d'anniversaire	89,10%
Sexe	81,54%
Parcours universitaire	31,91%
Styles de musique	31,11%
Réseaux	29,76%
Activités	28,35%
Films préférés	27,91%
Centres d'intérêt	24,86%
Livres préférés	22,85%
Opinions politique	17,94%
Parcours professionnel	17,47%
Site web personnel	7,58%
Orientation sexuelle	0,76%
Religion	0,65%

Durant le développement de l'application sociale, nous n'avons constaté aucune phase de validation venant des équipes Facebook. L'application a pu être diffusée sans aucune vérification ; pourtant bon nombre d'informations personnelles sont récoltées sans raison fonctionnelle. Cependant, nous avons malgré nous pu tester la réaction de Facebook sur une application face aux plaintes des utilisateurs. En effet, une anomalie dans l'application sociale que nous avons développé affichait une rafale de messages sur les murs des utilisateurs qui perdaient des amis dans un laps de temps plus grand que 5 minutes. Ainsi, les amis des utilisateurs avaient leur fil d'actualités pollués par de nombreux messages provenant de l'application. Notre application a été supprimée par Facebook sans nous prévenir ni nous

en informer. Nous pouvons donc supposer que les utilisateurs atteints par les messages polluants ont utiliser l'option « signaler cette application » disponible sur toute les applications du réseau et permettant de se plaindre du comportement d'un programme tiers. La réaction de Facebook a été très courte : environ 24 heures. Ainsi, notre application sociale n'était plus disponible, et tous ses utilisateurs ne pouvaient plus l'utiliser. Cependant, Facebook n'empêche pas aux développeurs malveillants de recréer leur application ; la seule contrainte est de changer l'adresse du canevas, qui a été mise sur liste noire. Cette mesure est bien sûr inefficace, car le changement d'une seule lettre suffit à pouvoir rétablir une application.

4.5 Conclusion

Nous avons vu comment concevoir une application sociale en prévoyant dès le départ la manière dont elle sera diffusée. Cette étude préalable est nécessaire pour assurer une ample propagation à une application. Les plates-forme de réseaux sociaux offrent des API extrêmement riches et qui mettent à la disposition des développeurs des fonctionnalités pouvant être exploitées pour augmenter la diffusion des applications, notamment en terme de communication avec les utilisateurs (messages, mur, notifications, invitations, etc.). L'utilisation de comptes fictifs comme base de diffusion est sans doute la technique la plus efficace, pour peu que les comptes soient correctement créés, de manière à attirer le plus de contacts possibles. Cette technique est bien évidemment à déconseiller dans le cadre d'une application sociale à vocation publicitaire pour une entreprise, mais elle peut être redoutable pour des développeurs malveillants souhaitant récolter un maximum d'informations personnelles sur les utilisateurs. Il est nécessaire de faire extrêmement attention aux informations que diffusent les employés d'une société sur ce type de réseaux. En effet, nous avons ciblé avec nos comptes fictifs des personnes provenant d'universités et d'entreprises diverses et variées, mais il serait très simple de cibler uniquement les employés d'une société précise, afin de retirer des informations personnelles qui pourront servir à des activités malveillantes.

5 Quelques Recommandations

5.1 Introduction

Nous avons vu que l'utilisation de réseaux sociaux par les employés d'une entreprise peut-être la cause de différents problèmes liés à sécurité :

- Propagation de *malwares*,
- Fuite de données personnelles, voire confidentielles,
- Mise à disposition d'informations utiles à l'ingénierie sociale.

Interdire tout usage des réseaux sociaux serait difficilement applicable, et inciterai les personnes concernées à trouver des moyens de contournement qui engendreraient des problèmes bien plus graves. Il est donc nécessaire de faire le point sur la manière dont peuvent être utilisés les réseaux sociaux au sein des sociétés, notamment en identifiant et en maîtrisant les risques. Bien qu'il n'existe pas de solution miracle pour prévenir ce nouveau type de risques, quelques idées de bon sens permettent à une politique de sécurité d'entreprise d'apprivoiser les réseaux sociaux. Nous verrons ainsi dans cette partie comment former le personnel d'un société à l'usage de ces réseaux, et comment bloquer uniquement ce qui est vraiment dangereux et qui ne peut être contrôlé : les applications sociales tierces. Enfin, nous étudierons comment utiliser les réseaux sociaux à notre avantage dans le cadre du métier de l'entreprise.

5.2 Former le Personnel

La meilleure manière de maîtriser l'usage des réseaux sociaux est sans doute la plus simple : comprendre leur fonctionnement, leurs limites et former les personnes amenées à s'en servir. Former le personnel est en effet aisé à mettre en œuvre et permet de donner quelques notions d'hygiène informatique plutôt que de tenter de tout interdire. Le premier point à aborder lors d'une telle formation est la description des risques apportés par les réseaux sociaux : une simple recherche sur un moteur de recherche permet de retracer le parcours professionnel d'une personne et d'identifier ses collaborateurs. Ces données ne sont pas confidentielles à proprement parler, mais leur accès est aujourd'hui si simple qu'il permet à un concur-

rent d'identifier les employés centraux d'un projet sensible, ou à une fausse agence de chasseurs de têtes de déstabiliser une activité.

Toutes ces informations n'ont pas nécessairement à apparaître sur le profil de quelqu'un. En tout cas, elles ne doivent pas être accessibles à tout le monde ; c'est pourquoi les paramètres de confidentialité des plates-forme sociales existent [9]. En effet, des efforts sont faits par les équipes des différents réseaux sociaux pour donner à leurs utilisateurs les outils suffisant pour contrôler les accès à leurs données personnelles. Par exemple, les centres d'intérêts d'une personne peuvent être configurés pour être visibles par tout le monde, par les amis de leurs amis uniquement, ou par leurs amis uniquement. En règle générale, il n'y a aucune raison de mettre un accès public à une information. La présence même du profil doit être cachée, de manière à ce qu'une requête sur un moteur de recherche à partir d'un couple nom / prénom ne renvoie aucune page provenant d'un réseau social. Dans la mesure du possible, il est important de ne renseigner que les informations utiles pour un profil, et d'en limiter l'accès aux amis seulement.

Ces précautions perdent de leur intérêt si l'utilisateur accepte tout le monde en tant qu'ami. Comme nous l'avons vu, accepter d'ajouter quelqu'un à sa liste d'amis donne à cette personne l'accès à toutes nos données ; dans le cadre d'une démarche d'ingénierie sociale de la part d'un concurrent ou de toute autre personne malveillante, ceci peut s'avérer compromettant. Toute demande de mise en relation doit donc être soigneusement étudiée. Hélas, se limiter à n'accepter que les personnes que l'on connaît ne suffit pas ; il est en effet simple pour une personne malveillante de créer le profil d'une personne que l'on connaît, ne serait-ce qu'en croisant les données de plusieurs réseaux sociaux. Il est donc nécessaire de s'assurer qu'une personne est bien qui elle prétend être, en entamant une correspondance avant tout acceptation.

Enfin, les réseaux sociaux permettent l'utilisation de listes, dont le principe général et de limiter l'accès aux données uniquement à certaines personnes faisant partie de la liste d'amis. Typiquement, au moins trois listes devraient être maintenues :

- La liste des collaborateurs professionnels,
- La liste de personnes de la famille,
- La liste des amis, en dehors des deux catégories précédentes.

Si ces listes sont fastidieuses à maintenir (à chaque nouveau contact doit être assigné une liste), elles permettent de contrôler qui voit quoi sur un profil. Par exemple, les photos des vacances de noël ne concernent en rien les collègues du bureau ; et certains messages ne doivent peut-être n'être lus que par certains amis. Ces listes permettent d'éviter le mélange de la vie personnelle et de la vie professionnelle, ce qui est le risque le plus important apporté par les réseaux sociaux.

5.3 Bloquer les Applications non Contrôlées

Bien que la formation du personnel est un point central de la gestion des risques des réseaux sociaux, elle ne permet pas d'éviter tous les problèmes. En effet et comme nous l'avons vu, personne ne peut savoir ce que fait une application tierce d'un réseau social, qui se confond souvent avec la plateforme officielle. La plupart du temps, ces applications sociales n'ont qu'un intérêt discutable dans le cadre professionnel : jeux vidéos, devinettes, jeux de rôles, etc. Si le blocage des réseaux sociaux sur les postes des employés d'une société semble inutile et difficile à mettre en place, le blocage de ces applications sociales est en revanche une bonne méthode pour éviter la fuite d'informations et le téléchargement de *malwares* à l'insu de tous. La plupart du temps, les applications sociales ont une adresse web commune facilement identifiable et qui permet leur filtrage sur un réseau. Par exemple sur Facebook, les canevas de toutes les applications tierces ont une adresse de la forme :

```
http://apps.facebook.com/<application_name>/
```

Ce format commun permet la mise en place de règles de filtrages dans un serveur mandataire web d'entreprise. De telles règles garantissent que les employés pourront utiliser les fonctionnalités officielles des réseaux sociaux sans pouvoir accéder aux applications tierces dont le fonctionnement peut être malveillant. Voici un exemple de règle utilisable sur le serveur mandataire le plus répandu : Squid.

```
acl facebook_apps dstdomain apps.facebook.com
http_access deny facebook_apps
http_access allow all
```

Bien sûr, les employés auront toujours accès à ces applications depuis l'extérieur de l'entreprise, mettant ainsi leurs données à disposition de personnes malveillantes ; c'est pourquoi la formation est nécessaire dans tous les cas.

5.4 Les Réseaux Sociaux au Service de l'Entreprise

Nous sommes désormais convaincus des risques apportés par les réseaux sociaux au sein d'une entreprise. Cependant, il est possible de tourner la richesse de ces plates-forme à l'avantage de l'entreprise. Les possibilités sont nombreuses, et toute sorte d'utilisation est envisageable. Nous allons exposer ici quelques idées pour faire en sorte que les réseaux sociaux ne soient plus un ennemi, mais un précieux allié.

Tout d'abord, les fonctionnalités offertes par les API des réseaux sociaux sont l'occasion de créer des applications à but publicitaire permettant de cibler une clientèle bien précise parmi les utilisateurs des plates-forme sociales. Une application amusante et correspondant bien à sa cible d'utilisateurs peut se diffuser à grande échelle, d'ami en ami par le bouche-à-oreille ou par les méthodes de diffusion que nous avons étudié précédemment. Si cette application sociale intègre votre société en tant que sponsor de manière cohérente, l'image de marque de votre entreprise peut gagner en popularité [10]. La société Groupama a bien compris comment exploiter cette richesse en créant une application qui a su attirer un public amateur de voile ou de mini-jeux. Cette application sociale a remporté un franc succès, avec plus 17500 utilisateurs actifs par mois.

Si une application à usage externe permet de véhiculer une image de marque, une application à usage interne permet de contrôler l'utilisation faite par les employés des réseaux sociaux. Pourquoi ne pas autoriser l'utilisation des réseaux sociaux dans l'entreprise à condition de signer une charte d'utilisation dédiée et d'installer sur son profil une application de contrôle ? Cette application de contrôle, développée en interne, permettrai par exemple de vérifier à intervalle régulier l'état des autorisations d'accès attribuées par chaque employé à ses données personnelles. Sans faire de « flicage », cette application n'aurait pas pour but se suivre l'activité des employés sur les réseaux sociaux, mais simplement de lever une alerte lorsqu'une

donnée personnelle est accessible à tout le monde alors qu'il serait préférable de la dissimuler. Bien évidemment, une telle application devra être présentée dans sa globalité aux employés, afin qu'ils en comprennent les tenants et les aboutissants et l'acceptent. Enfin, il est possible de tirer parti de l'indiscrétion impliquée par les réseaux sociaux. En effet, il y a fort à parier qu'une entreprise figurant parmi vos clients potentiels ai des employés utilisant un réseau social. Il s'agit là d'une occasion simple et rapide de trouver un nom et démarrer une opération commerciale. Dans le même ordre d'idées, plutôt que de passer par d'onéreux chasseurs de têtes, les réseaux sociaux sont parfois un outil puissant pour trouver des personnes compétentes et expérimentées dans votre secteur d'activité.

6 Conclusion

Il est de fait que les réseaux sociaux posent quelques problème relatifs à la sécurité dans le cadre d'une entreprise. Ceci est essentiellement du au fait que leur apparition s'est faite brutalement, et que leur taux d'utilisation a augmenté de manière fulgurante, sans que les politiques de sécurité ne puissent suivre. Les employés ont pris de nouvelles habitudes que les règles organisationnelles ne prennent pas toujours en compte. Mais des pratiques simples permettent de rétablir la confiance : formation et interdiction minimales étant les principes fondamentaux. Il est également possible de profiter de l'existence des réseaux sociaux plutôt que de la subir. La richesse fonctionnelle et sociale qu'ils apportent peut être exploitée pour la promotion d'un produit, d'un concept, voire d'une image de marque. Il serait dommage de s'en priver.

Références

1. Winder, D. : Being virtual : who you really are online. John Wiley & Sons Ltd. p. 211 (2008)
2. Jakobsson, M., Ramzan, Z. : Crimeware : Understanding New Attacks and Defenses. Symantec Press pp. 55–77 (2008)
3. Baltazar, J., Costoya J., Flores, R. : The Real Face of KOOBFACE : The Largest Web 2.0 Botnet Explained. Trend Micro Threat Research (2009)
4. IT Governance Research Team : How to Use Web 2.0 and Social Networking Sites Securely. IT Governance Publishing p. 10 (2009)

5. Athanasopoulos, E., Makridakis, A., Antonatos, S., Antoniades, D., Ioannidis, S., Anagnostakis, K. G., Markatos, E. P. : Antisocial Networks : Turning a Social Network into a Botnet. Foundation for Research & Technology Hellas (2008)
6. Graham, W. : Facebook API Developers Guide. Apress pp. 20–28 (2008)
7. Fogg, B. J., Iizawa, D. : Online Persuasion in Facebook and Mixi : A Cross Cultural Comparison. In : Persuasive Technology : Third International Conference, Springer pp. 35 –46 (2008)
8. Bitan, H. : Droit des créations immatérielles. Lamy p. 120 (2010)
9. Fong, P. W. L., Anwar, M., Zhao, Z. : A Privacy Preservation Model for Facebook-Style Social Network Systems. In : ESORICS 2009 14th European Symposium on Research in Computer Security, Springer pp. 303–320 (2009)
10. Rutledge, P.-A. : The Truth about Profiting from Social Networking. FT Press pp. 87–103 (2008)