Applications Facebook : Quels Risques pour l'Entreprise ?

François-Xavier Bru[1] Guillaume Fahrner[1] Alban Ondrejeck[2]

[1]Mastère Spécialisé en Sécurité des Systèmes d'Information, Télécom Bretagne
{fx.bru,guillaume.fahrner}@telecom-bretagne.eu

[2]Orange Consulting alban.ondrejeck@orange-ftgroup.com

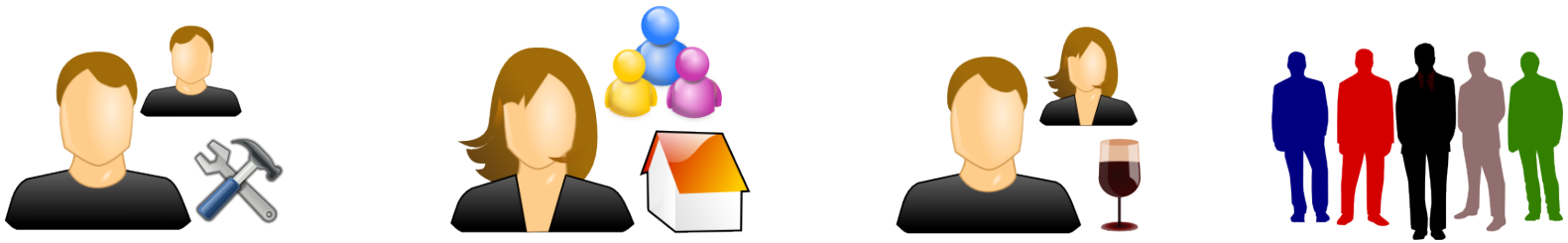
10 juin 2010

Agenda

Introduction

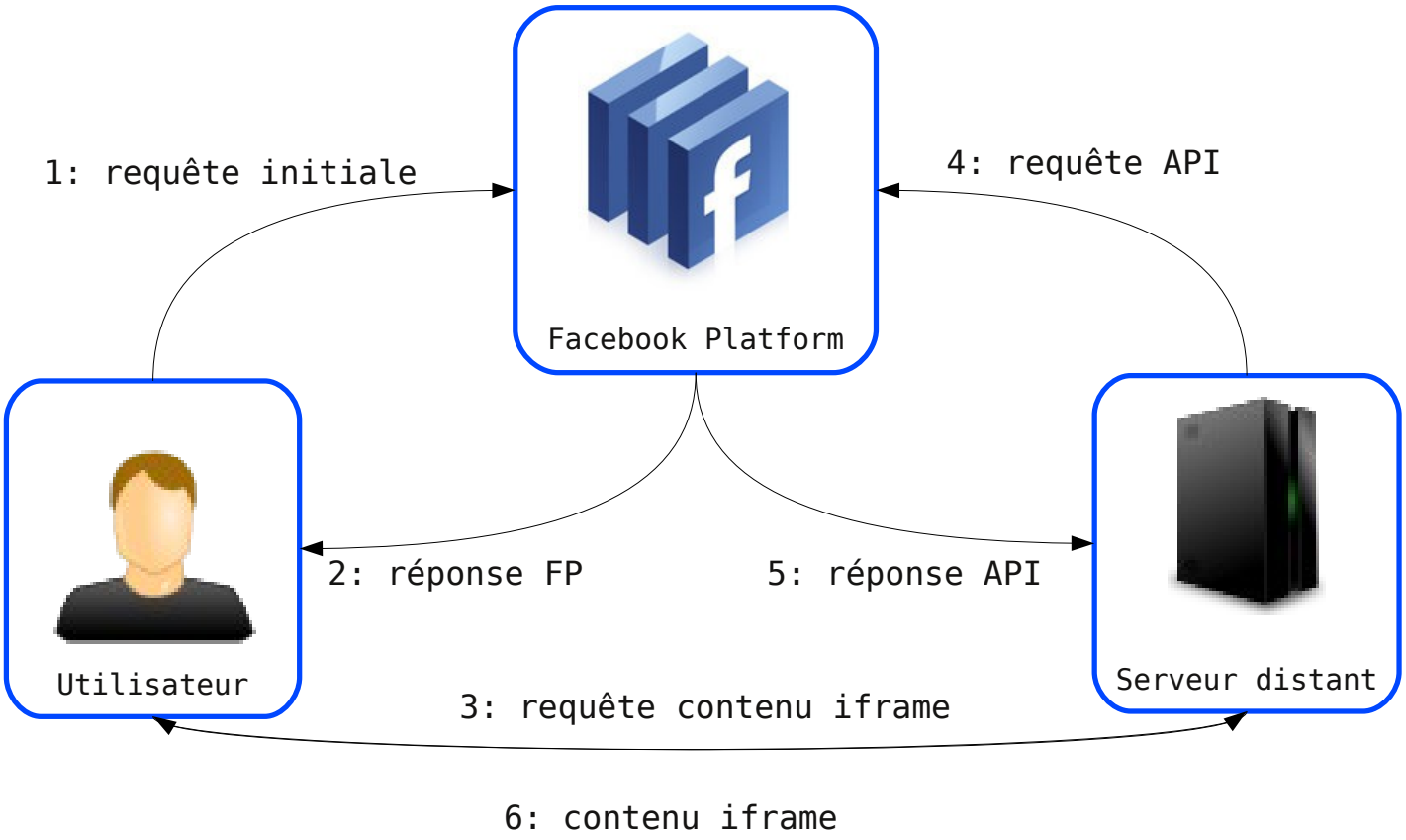
Un succès croissant

Des utilisateurs variés



Une nature favorisant les échanges

Une Plate-Forme de Développement Peu Sécurisée

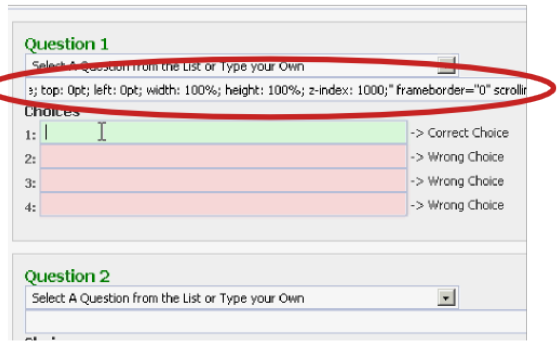


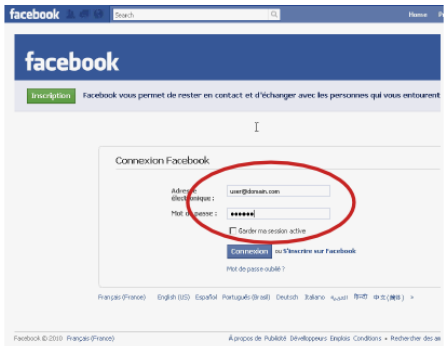
Des Applications Vulnérables

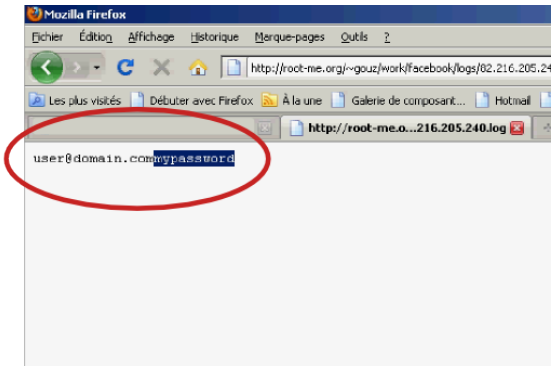
Constat

Trop d'applications pour permettre une validation de leur sécurité.

Injection SQL, modification HTTP/POST, XSS, etc.







Combien d'autres applications populaires sont vulnérables ?

Des Applications Malveillantes

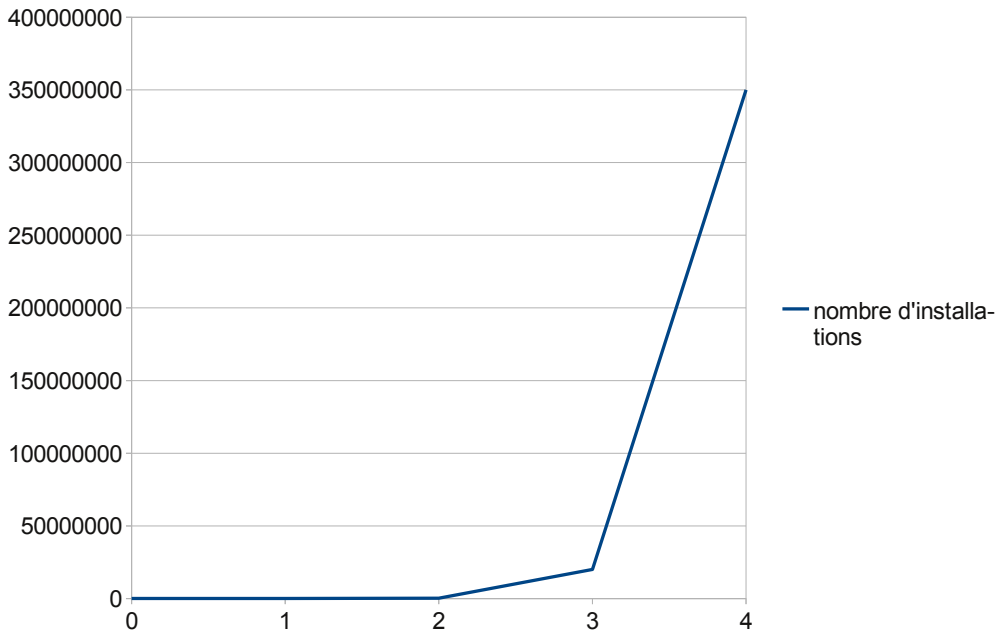
Constat

Trop d'applications pour vérifier si elles sont malveillantes ou non.

Combien d'applications sont malveillantes sans que personne ne le sache ?

Diffusion d'une Application

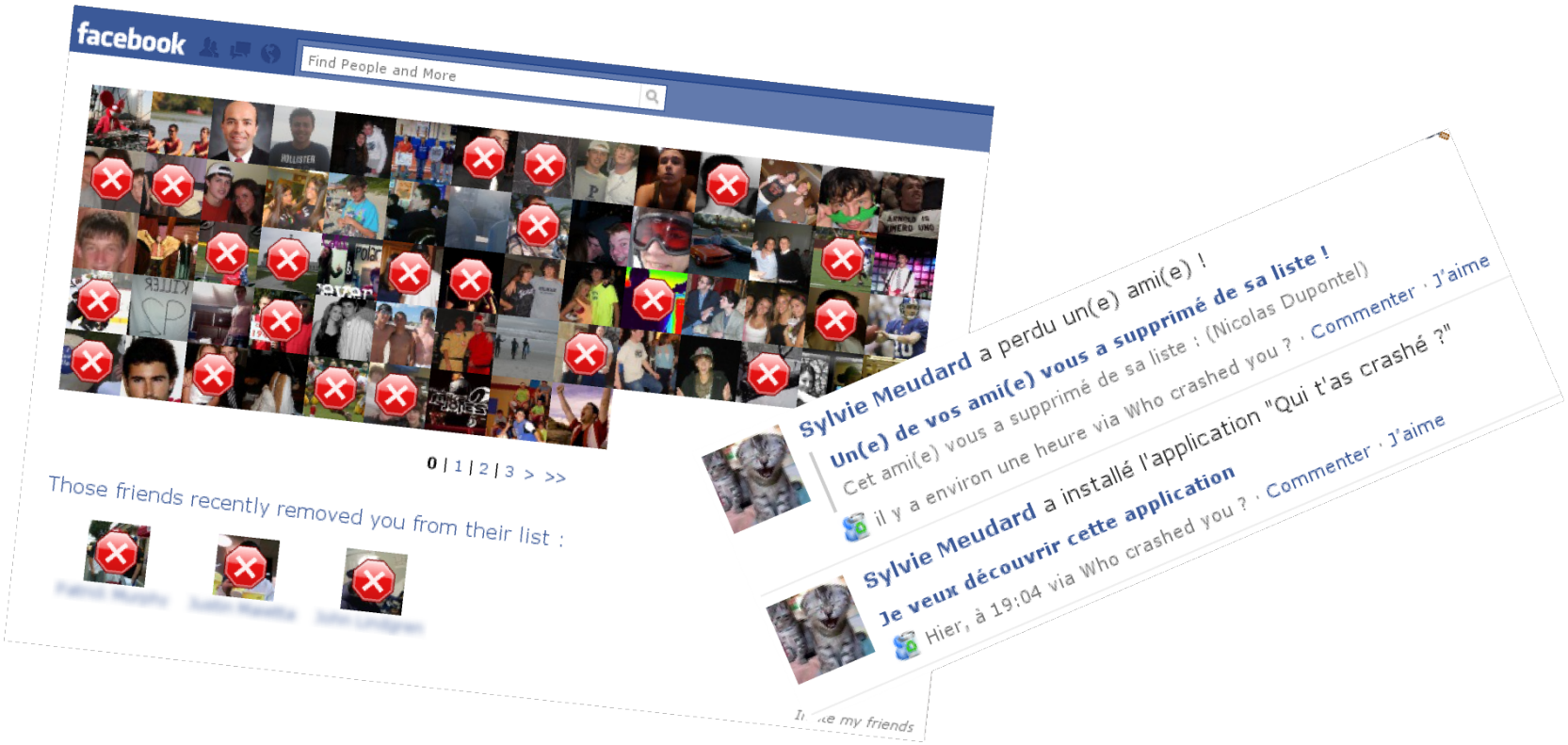
- Une bonne diffusion peut être utile à :
  - Une entreprise, dans un but commercial
  - Un attaquant, pour toucher un maximum d'utilisateurs
- Les possibilités offertes par Facebook sont impressionnantes



Principe de la Stratégie de Diffusion

- Primordiale en amont du développement
  - Que cherche-t-on à faire ?
  - Pourquoi veut-on le faire ?
  - Comment va-t-on le faire ?
- Définit la cible à atteindre
  - Victimes ou clientèle potentielle ?
  - Centre d'intérêts ?
  - Tranche d'âge ?
- Dans le cas de notre étude :
  - But : récolter un maximum de données personnelles
  - Comment : relayage social (murs, notifications)
  - Cible : le plus de monde possible
    - Entre 15 et 25 ans
    - Francophones
    - Anglophones
  - Fonctionnalités : utiles et amusantes

Who Crashed You ?



Création de Profils Fictifs

- Profils fictifs comme "rampe de lancement"
- Caractéristiques dépendantes de la stratégie de diffusion
- Les mécanismes sociaux de Facebook permettent de :
  - Repérer les cibles selon une tranche d'âge, un parcours, des intérêts
  - D'envoyer rapidemment des ajouts à la liste d'amis (sans CAPTCHA)
  - Bénéficier d'un effet boule de neige grâce aux amis communs
- Dans le cadre de notre étude :
  - 21 profils fictifs créés
  - 5043 demandes envoyés
  - Taux de retour de 38,6%

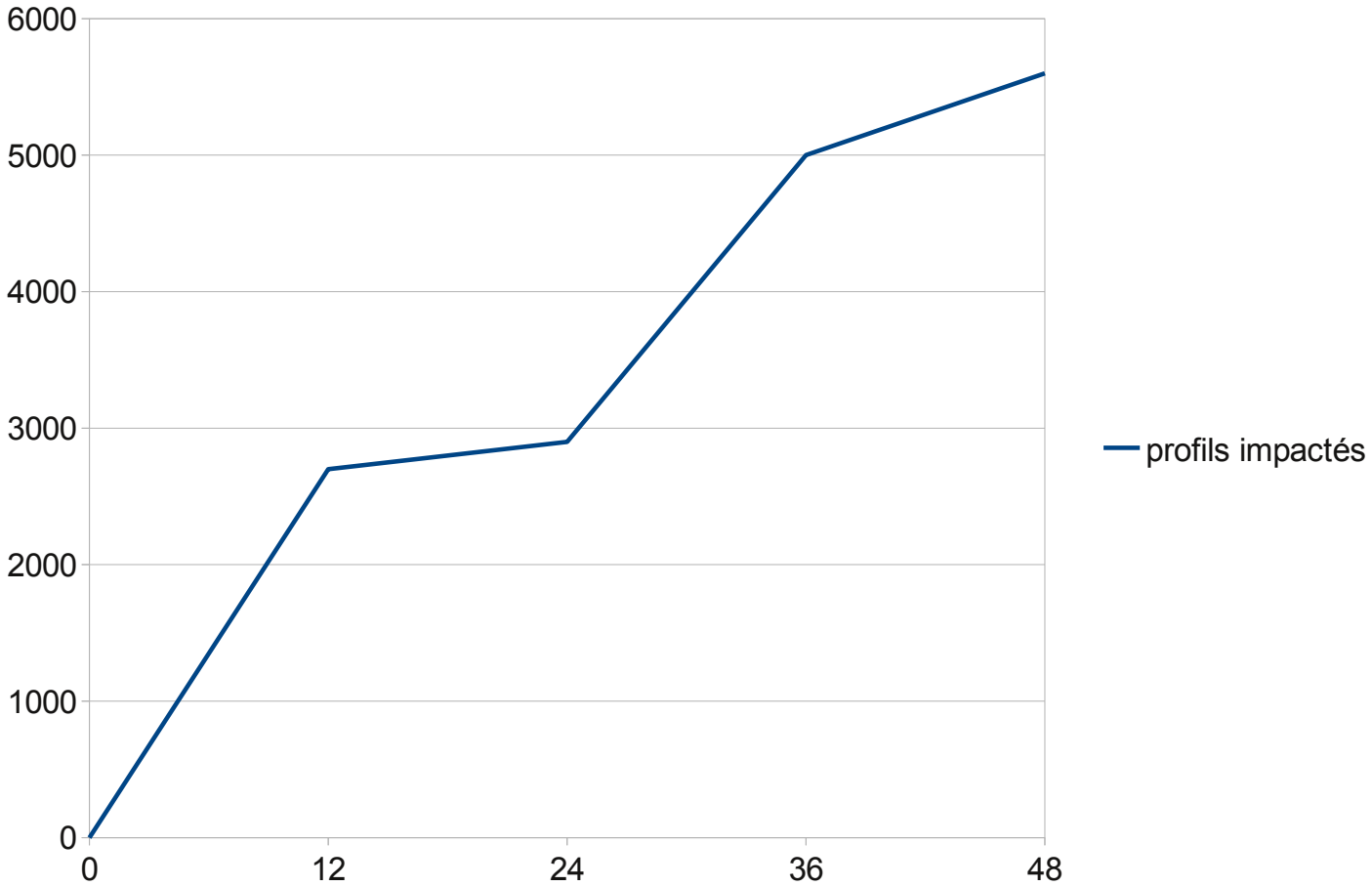
Efficacité des Profils Fictifs

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

Citation représentative

"On a dû se côtoyer, vu la proximité de nos parcours", *Allain A.*

Courbe d'Evolution



Données Récoltées

Type d'informations	Récolte
Date d'anniversaire	89,10%
Centres d'intérêt	24,86%
Opinions politique	17,94%
Parcours professionnel	17,47%
Orientation sexuelle	0,76%
Religion	0,65%

Réaction de Facebook

- Aucun contrôle pendant le développement
- Aucun contrôle pendant la diffusion
- Manifestation seulement après réaction des utilisateurs (*signaler cette application*)
- Aucune sanction définitive, possibilité de recréer une application identique avec un autre nom
- Base de signatures des applications malveillantes ?

Quelques Recommandations

- Les réseaux sociaux apportent de nouveaux risques
- Les politiques de sécurité doivent être adaptées
- Tout interdire ?
  - Difficile d'un point de vue relationnel
  - Difficile à mettre en place (proxys web)
  - Incite à contourner la politique de sécurité
- Le point central est la formation
  - Quels sont les risques des SN ?
  - Qui peut accéder à vos données ?
  - Comment paramétrer son profil ?
  - Éviter les contacts inconnus
  - Éviter les applications tierces
- Utiliser les applications à son avantage ?

Conclusion

Les réseaux sociaux sont effectivement dangereux :

- Ils forment de nouveaux vecteurs de propagation de malwares
- Les utilisateurs gèrent mal leurs données personnelles
- De nombreuses attaques sont possibles, notamment par les applications tierces

Mais ces dangers sont plus faibles qu'on ne le pense :

- Un minimum de sensibilisation écarte la plupart des risques
- Diffuser une application malveillante n'est pas si simple...
- Il est possible de tourner ces réseaux à l'avantage de l'entreprise

Références

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

Références

- Graham, W. : *Facebook API Developers Guide.* Apress pp. 20–28 (2008)
- 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)
- Bitan, H. : *Droit des créations immatérielles.* Lamy p. 120 (2010)
- 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)
- Rutledge, P.-A. : *The Truth about Profiting from Social Networking.* FT Press pp. 87–103 (2008)

Questions