Le Rôle des Hébergeurs Dans la Détection de Sites Web Compromis

Davide Canali, Davide Balzarotti, Aurélien Francillon

Software and System Security Group

EURECOM, Sophia-Antipolis

*Publié à la conférence WWW'13

Motivations

EURECOM
Sophia Antipolis

- **Hébergement mutualisé**
  - Millions d'utilisateurs
  - Sites web pour particuliers et petites entreprises
  - Utilisateurs avec peu de connaissances en sécurité
  - Même un utilisateur expérimenté a ni visibilité ni contrôle
- **Grande surface d'attaque potentielle**!

- Les hébergeurs devraient jouer un rôle important pour assister leurs clients en cas d'attaque
  - Est-ce le cas?

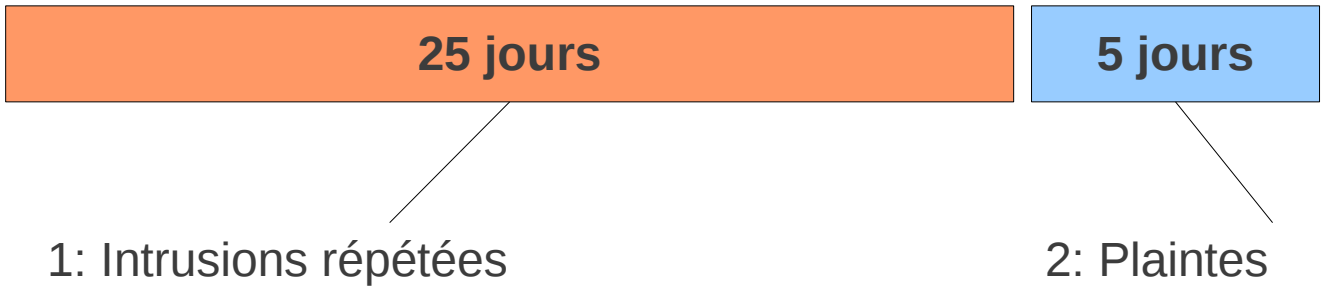
Méthode de test (1/2)

EURECOM
Sophia Antipolis

- **Achat** de plusieurs hébergements mutualisés
- Installation de applications web open source
- Simulation de différents «scénarios d'intrusion»
- **Tests** étudiés afin d'être facilement **détectables**
  - et de ne pas mettre en danger l’hébergeur ou des visiteurs potentiels

Méthode de test (2/2)

- Phase 1: attente de la réaction de l'hébergeur
- Phase 2: envoi de plaintes concernant nos sites web
  - **Plaintes légitimes** concernant les attaque de phishing et fichiers malveillants
  - **Plaintes illégitimes** dénonciation de fichiers malveillants et de contenus offensants, contre un site web «propre»



Hébergeurs évalués

- **12** des principaux hébergeurs **mondiaux** (principalement aux États-Unis)
- **10** hébergeurs **régionaux**
  - Basés en Europe, US, Inde, Russie, Algérie, Hong Kong, Argentine, Indonésie
- 6 services de sécurité additionnels
  - Abonnement de moins de 30 $/mois
  - 10 jours de seuil de détection (on attend une réponse rapide d'un service dédié)

Scénarios

EURECOM
Sophia Antipolis

- Infection par un botnet
- Vol de données (via SQL injection)
- **Kit de phishing**
- Inclusion de code malveillant (drive-by-download)
- **Identifiants volés (upload de fichiers malveillants)**

- **5 tests * 22 hébergeurs = 110 tests**

Remote File Upload d'un kit de phishing

EURECOM
Sophia Antipolis

Installation

- OsCommerce reproduisant une vulnérabilité **Remote File Upload** connue

Attaque

- *Phase d'attaque*, toutes les 6 heures: upload d'un vrai **kit de phishing** en exploitant la vulnérabilité d'OsCommerce
- *Phase victime,* tous les 15': simule une victime du phishing
  - Les champs des page de phishing sont remplis avec données factices mais réalistes (ex. N° carte de crédit « correct »...)

Identifiants volés
(upload de fichiers malveillants connus)

EURECOM
Sophia Antipolis

Installation

- Page HTML statique avec phrases en Anglais et quelques images

Attaque

- **Upload** de deux **fichiers malveillants** sur le site
  - par **FTP** (mot de passe volé)
- Détectés par la plupart des antivirus
  - *c99.php*: shell web (c99)
  - *sb.exe*: Ramnit worm
- Toutes les 6 heures

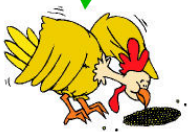
Organisation des tests

EURECOM
Sophia Antipolis

Compte sur serveur
d'hébergement mutualisé

Partie simulée

Attaquant
Tous les tests
groupe d'IPs "A"



Victime
Test *Phish*
groupe d'IPs "B"

Visiteurs
Visitent les pages de façon aléatoire
Tous les tests
groupe d'IPs "C"

Résultats: inscription

EURECOM
Sophia Antipolis

- Certains hébergeurs **découragent** les **inscriptions abusives ($$$)**
- Les **hébergeurs globaux** sont **plus attentifs** que les régionaux
- **Trois** hébergeurs **régionaux** ont une procédure d'**inscription très simple**

Résultats: prévention et détection

EURECOM
Sophia Antipolis

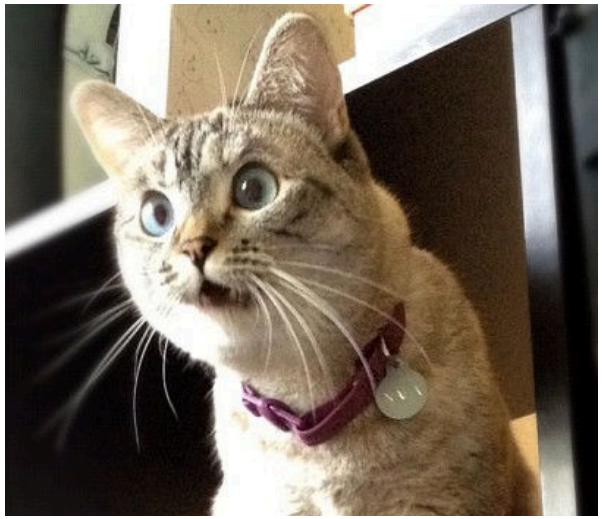
- Certains hébergeurs ont des mesures de **prévention:**
  - **Listes noires d'URLs (**SQL et File Uploads)
  - Seulement les attaques basiques bloqués (~30%)
  - Filtrage des connexions et au niveau du système

Résultats: prévention et détection

EURECOM
Sophia Antipolis

- Certains hébergeurs ont des mesures de **prévention:**
  - **Listes noires d'URLs (**SQL et File Uploads)
  - Seulement les attaques basiques bloqués (~30%)
  - Filtrage des connexions et au niveau du système

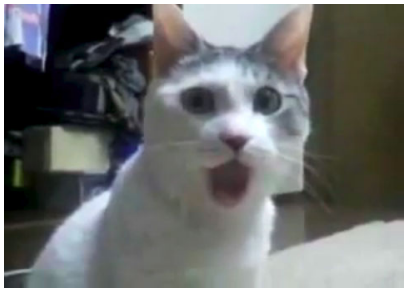
- **Détection:** résultats **décevants**
  - **Un seul hébergeur** a été capable de détecter **une attaque**
  - Alerte pour le **test AV reçue 17 jours après** son lancement



Résultats: plaintes

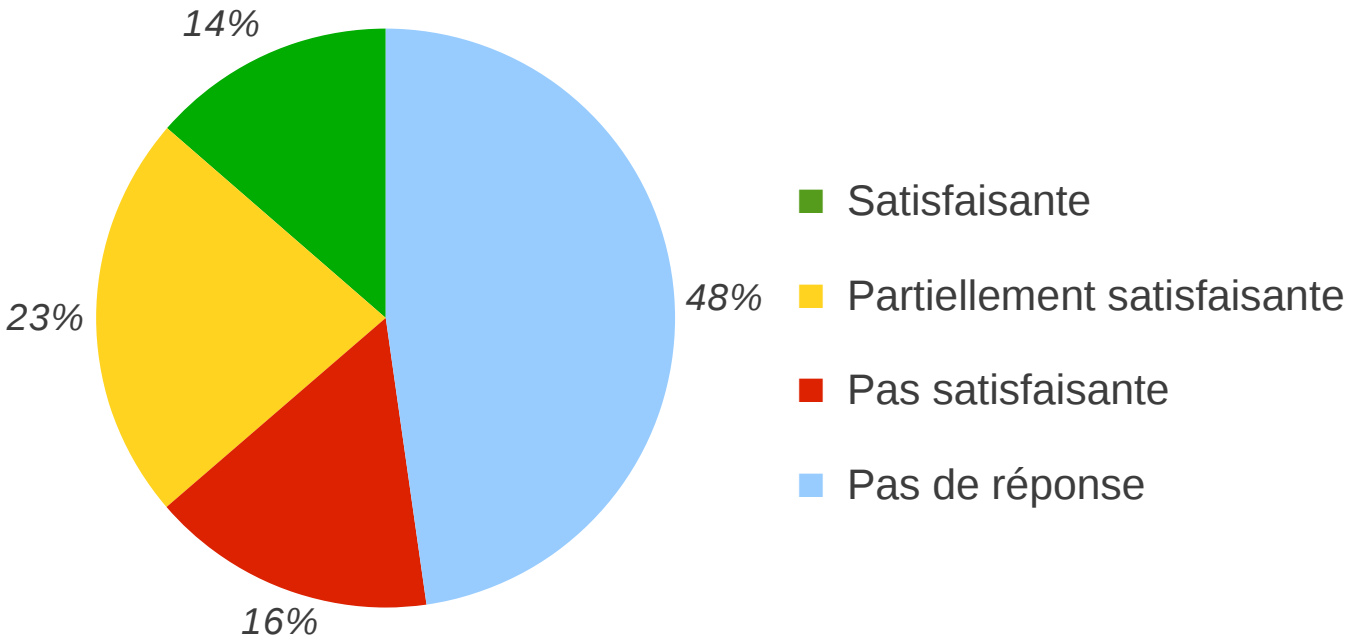
EURECOM
Sophia Antipolis

- **50%** des hébergeurs n'ont **jamais répondu**



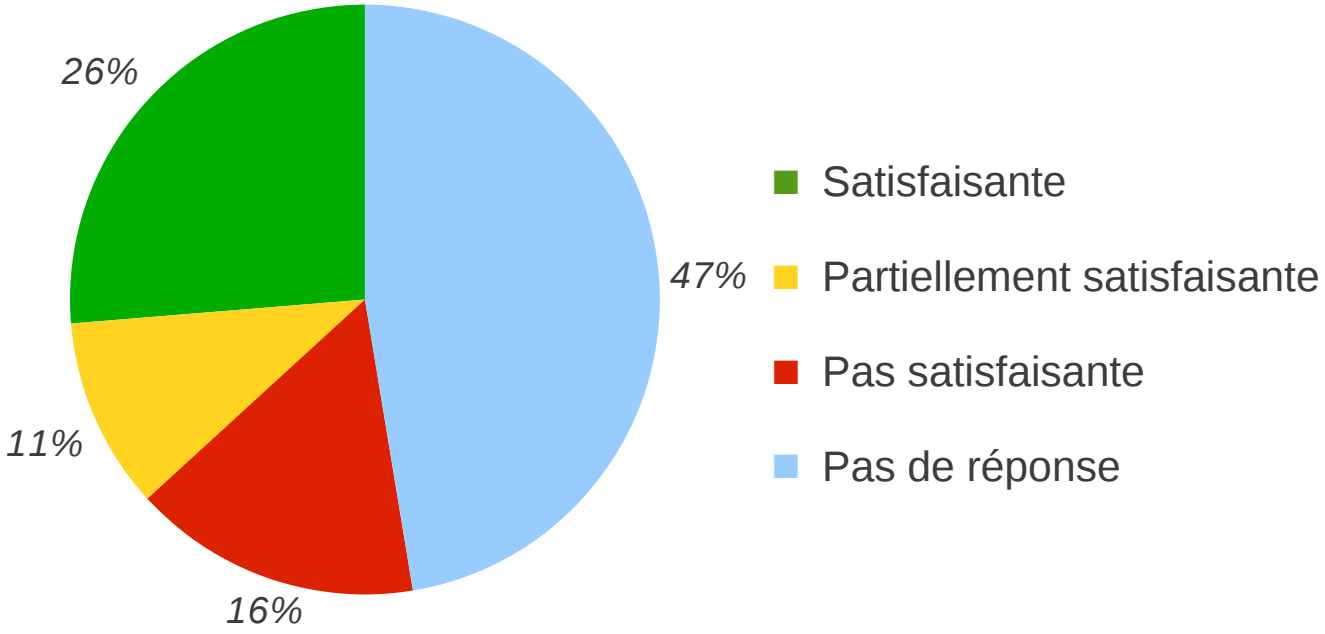
- **64%** des **réponses** reçues **dans la journée** suivant l'envoi de la plainte
- Temps de réponse moyen:
  - **28h** pour hébergeurs **globaux**
  - **79h** pour les **régionaux**
- Grande variété de réactions ...

Réponse aux plaintes légitimes



- **Seulement 3** hébergeurs **sur 22** réagi correctement
- Certains ont eu une trop forte réaction (ex., clôture du compte)
  - D'autres ont envoyé un ultimatum à l'usager mais n'ont pas contrôlé si le compte avait été nettoyé

Réponse aux plaintes illégitimes

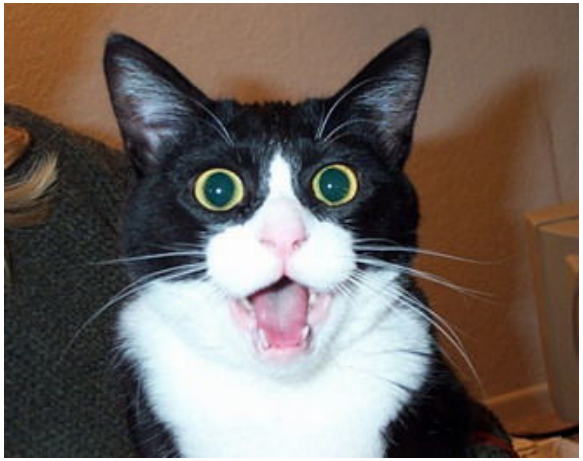


- Au Plus **14** hébergeurs **sur 19** ont bien répondu
- **3** hébergeurs (régionaux) ont **réagi aux plaintes** sans contrôler!
  - Mauvaise réaction (ex., compte suspendu, effacement de fichiers)
  - Alors que les sites étaient propres

Détection par services de sécurité complémentaires

EURECOM
Sophia Antipolis

- **Cinq** services **sur six** n'ont **rien détecté**



- Un a détecté
  - Les fichiers malveillants (scan antivirus) mais ils n'ont **pas informé l'utilisateur**
  - Une **page** contenant du code malveillant

Conclusions

EURECOM
Sophia Antipolis

- Beaucoup d'**efforts** pour **prévenir inscriptions frauduleuses**
- La plupart des hébergeurs utilisent des **moyens basiques** pour **prévenir les attaques simples** (ex., blacklists d'URLs)
- **Aucun effort** pour la **détection** de **signes évidents de compromission**
- **Services de sécurité** pas chers **ne servent à rien**
- **La moitié des hébergeurs répondent** aux plaintes
  - 14% seulement de façon approprié

Merci!

EURECOM
Sophia Antipolis

?

Pour questions, conseils, commentaires

canali@eurecom.fr