ARKOON NETWORK SECURITY

Argumentaire
Antispam FAST360

1. **Définition et histoire du spam**
2. **Les risques liés au spam**
3. **Les principales techniques antispam**
4. **Pourquoi choisir l'antispam des appliances FAST360**
5. **Le traitement des objections types**

1. Définition et histoire du spam

Le 12 avril 1994, le premier SPAM, envoyé à plusieurs dizaines de milliers de destinataires pour faire connaître la société de conseil de 2 juristes américains, Laurence Canter et Martha Siegel, a rapporté un revenu direct estimé à 200 000 $...

Depuis son origine, la seule motivation des spammeurs est la rémunération qu'ils peuvent tirer du spam :

- Rémunération au "clic" sur les sites d'annonceurs.
- Vente de la base des adresses qui répondent au spam.
- Vente en ligne de produits et services présentés dans le spam.
- Arnaques diffusées par le spam.

Aujourd'hui ce sont les organisations de grand banditisme qui engrangent, grâce au spam, des sommes colossales. Ces mafias optimisent leurs revenus et leur impunité en embauchant des hackers :

- Les virus créent des réseaux "zombies" qui vont démultiplier les attaques par spams en masquant l'identité des spammeurs
- Intégration d'images (2006), spam MP3 (2007)….
- Le volume de Spam a augmenté pour atteindre 120 milliards de messages par jour
- Recours à des stratagèmes pour conférer aux messages un semblant d'authenticité : dissimulation d'URL dans des résultats de recherche, insertions de lien dans des contenus transactionnels…

2. Les risques liés au spam

Saturation des infrastructures

- Engorgement des réseaux avec des impacts sur la consommation de bande passante.
- Charge supplémentaire sur les dispositifs de stockage et les serveurs de messagerie.

Perte de productivité

Temps perdu par les destinataires à :

- Trier et effacer les spams.
- Chercher à identifier les émetteurs.
- Se désabonner des listes de diffusion.
- Consulter les sites sur lesquels le spam redirige les Internautes.

Menaces diffusées par spam

Les spams servent souvent de moyen de diffusion à d'autres menaces :

- Virus
- Vers
- Phishing : un mail qui semble émaner d'une organisation de confiance (banque, société de Ebusiness…) et qui redirige en fait les destinataires vers un faux site Web, sur lequel on leur soutire de l'argent.

Perte de messages utiles

Le spam crée un bruit de fond dans la boite aux lettres des utilisateurs. Noyés dans la masse des spams, les mails importants peuvent être ignorés voire effacés par les utilisateurs.

Risque juridique
Il est de la responsabilité d'une société et de son chef d'entreprise de protéger ses salariés contre les contenus parfois choquants des spams et de s'assurer qu'ils ne consultent pas des sites Web illicites (pédophiles, xénophobes…) sur lesquels peut les rediriger un spam.

Abandon d'adresse Email
Si une adresse Email est systématiquement spammée et que l'entreprise n'est pas en mesure de la protéger, la solution ultime est de supprimer cette adresse.

3. Les principales techniques antispam

Les filtres sur émetteur ou DNSBL :

- Bloquent les spams en se basant sur des listes noires de serveurs émetteurs.
- Nécessitent de faire confiance aux listes noires utilisées.
- Ne permettent pas de bloquer les spams émis depuis des serveurs non "blacklistés".
- Ne constituent plus une sécurité suffisante, devant le nombre colossal de spams.

Les filtres sur le contenu :

1. *Filtres heuristiques*
   - Des règles permettent d'analyser les contenus récurrents des spams (en-têtes, émetteur, destinataires, objet et corps du mail, balises HTML, scripts…)
   - Chaque règle à un score
   - A la fin de l'analyse, le score global du mail indique si c'est un spam.
   - Difficulté de reconnaissance des spams « images » ou MP3
   - Efficacité liée à la mise à jour en continu des règles

2. *Filtres sémantiques ou Bayesiens*
   - Se basent sur l'expérience du moteur qui donne sa propre définition des SPAMS et des bons mails (appelés HAMS).
   - A besoin d'être régulièrement entretenu pour être performant.
   - Nécessite un travail de correction, d'entraînement et de personnalisation par un destinataire.
   - Difficilement gérable au niveau d'une entreprise ou d'une passerelle.

Les filtres « Temps Réel »

- Des centres de détection utilisent des algorithmes d'analyse en temps réel du trafic mondial (des milliards de mails par jour) basés sur des critères indépendants du contenu : IP réputation, recurrent pattern detection, technique d'envoi…
- Pas de problématique de mise à jour
- Détection de tout type de contenu (Image, MP3…)
- Pas d'impact sur la performance
- Taux de faux-positifs quasi nul

4. Pourquoi choisir l'antispam des appliances FAST360 d'ARKOON

La performance

- Le moteur antispam « Temps Réel » des appliances FAST360 est 10 fois plus rapide qu'un moteur classique heuristique ou bayésien.
- Il est intégré à l'architecture SSA pour plus d'imbrication des technologies et donc plus de performance.

La baisse des coûts d'administration

- La configuration, la supervision et la mise à jour de toutes les fonctions de filtrage de contenu (antivirus, filtrage d'URL, antispam…) sont centralisées sur l'appliance FAST360.

La combinaison des technologies de filtrage sur le même équipement

- Si un nouveau virus est diffusé par spam, il est bloqué par l'antispam ARKOON avant que sa signature antivirale ne soit connue.
- Si un spam tente de diriger les utilisateurs sur un site de phishing, le filtrage d'URL les bloque.

5. Le traitement des objections types

Objections	Réponses
J'ai déjà une solution sur DNSBL, pourquoi payer une option supplémentaire ?	Les DNSBL ne suffisent plus à surmonter le problème du spam. Les spammeurs changent régulièrement de serveurs de diffusion et utilisent les serveurs « zombies » d'entreprises. Les DNSBL constituent une première barrière qui doit être renforcée par des solutions de filtrage « temps réel ».
Vos concurrents UTM intègrent aussi des solutions Antispam.	Non, tous nos concurrents proposent des solutions DNSBL qui sont chez nous intégrées nativement et sans coût additionel. Mais les appliances FAST360 sont parmi les seules à intégrer une solution de filtrage antispam de contenu.
Je préfère utiliser une solution de type Heuristique ou Bayesien, il y a moins d'erreur.	Les filtres bayesiens sont les plus personnalisables des filtres de contenu, mais pas les plus efficaces sur une solution d'entreprise. En effet, ils doivent être maintenus, entraînés, mis à jour, supervisés. Ce qui est très difficile à gérer pour un administrateur au niveau d'un filtre d'entreprise.
Avec votre solution, on ne peut pas gérer de quarantaine.	C'est faux, la solution Arkoon permet de gérer 2 niveaux de quarantaine : Une quarantaine dédiée à chaque utilisateur. Cela nécessite le paramétrage du client de messagerie de l'utilisateur pour stocker les spams dans un dossier dédié de sa boite mail. ET/ou une quarantaine globale. Pour cela, on redirige chaque spam vers une adresse mail paramétrable qui servira de quarantaine globale (disponible en 4.1).
Intégrer un AntiSpam sur une appliance multifonctions ? Les performances doivent être désastreuses !!!	Non car le moteur que nous utilisons a été développé dans un souci de performance. Aucun traitement ni analyse ne sont réalisés directement sur l'appliance.
Votre AntiSpam ne peut pas rendre le même service qu'une appliance dédiée.	C'est vrai, une appliance dédiée apporte forcément des fonctions supplémentaires par rapport à un produit UTM. Mais, en contrepartie, la solution Arkoon présente les avantages suivants : - elle est moins chère à l'achat (pas de coût matériel, pas de maintenance spécifique) - elle permet de réduire le nombre d'appliances (risque de panne plus faible) - elle permet de réduire les coûts d'administration (1 seule interface pour tous les services de sécurité) - elle est plus simple à mettre en œuvre - elle est plus efficace pour contrer de nouvelles menaces qui nécessitent la combinaison de plusieurs moteurs *(comme par exemple de nouveaux virus ou le phishing qui peuvent être arrêtés par la combinaison de l'IDPS, de l'antivirus, de l'antispam et du filtrage URL)*

Si votre Antispam laisse passer des spams c'est qu'il n'est pas efficace !	Il ne faux pas confondre virus et spam ! Si un seul virus peut faire des dégâts, c'est l'accumulation des spams qui est dangereuse. Donc la qualité d'un antispam ne se mesure pas uniquement sur son taux de détection, mais à sa capacité à réduire considérablement le nombre de spams en limitant le nombre de détections à tort (ou faux positifs) Un antispam qui bloque 100% des spams mais qui fait beaucoup de faux positifs est moins efficace qu'un antispam qui ne bloque que 80% des spams mais sans faire de faux positifs. **A ce titre, les tests réalisés par Arkoon sur son moteur « Temps Réel » montrent que le taux de détection est supérieur à 95% pour moins de 0,0001% de faux positif, ce qui le classe dans les meilleurs du marché.**
Je reçois plein de mails publicitaires, sont-ils reconnus comme spams !	Non, un mail publicitaire n'est pas un spam. Il est envoyé de façon légitime et autorisé à partir d'une liste de diffusion réglementé. Vous pouvez également vous désabonner de la liste de diffusion.