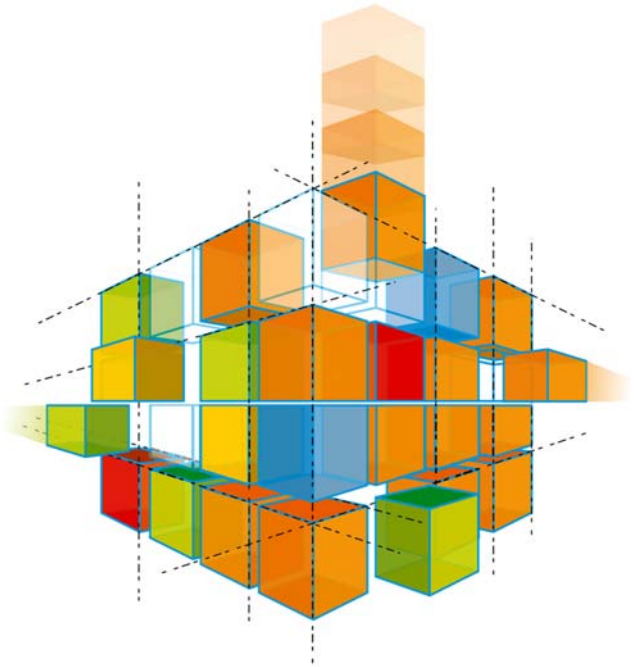
Arkoon Network Security

Migration Antispam



Technologie « Temps réel »
(Commtouch)

versus

Technologie Heuristique

ARKOON
NETWORK SECURITY

Moteur Antispam « temps réel »

Le spam, qui représente 70% du courrier électronique mondial, est devenu un véritable fléau.

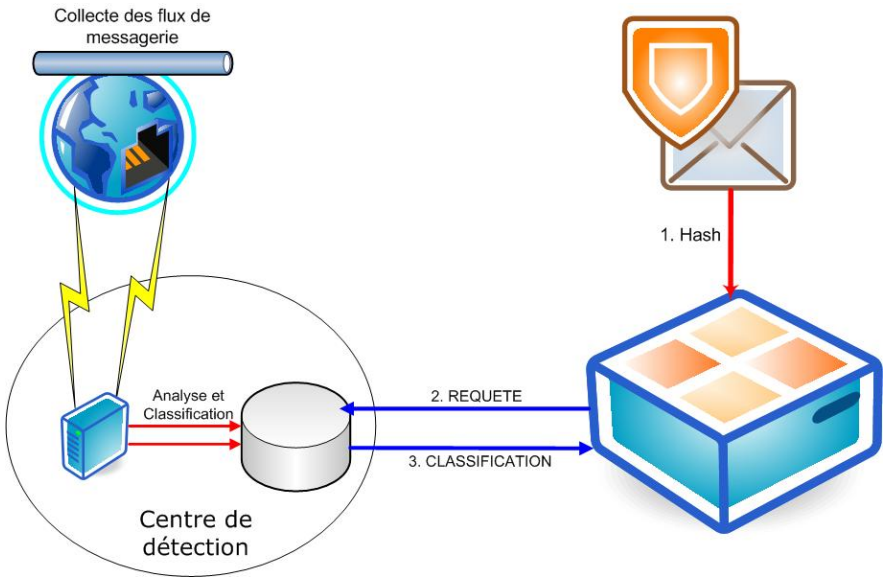
Les enjeux économiques sont tels que les moyens mis en œuvre par les « spammeurs » sont de plus en plus sophistiqués.

Les techniques à base de moteurs heuristiques (règles s'appuyant sur l'analyse du contenu) ou bayésiens (apprentissage) ne sont aujourd'hui plus assez satisfaisantes.

- en effet, ces moteurs ne sont efficaces qu'à la condition d'être systématiquement mis à jour avec de « nouvelles règles » dès la sortie d'une nouvelles vague de Spam.
- même si le taux de détection peut sembler correct, ces techniques engendrent alors des taux de faux-positifs (blocage du courrier légitime) inacceptables.

Moteur Antispam « temps réel »

Les appliances FAST360 embarque aujourd'hui un moteur « temps réel » issu de la technologie Commtouch RPD (Recurrent Pattern Detection).



Le mécanisme consiste à confronter une empreinte (hash) du mail à analyser à une base de données centralisée (Centre de Détection Commtouch) qui retourne instantanément, en temps réel, un statut.

FAST360

Moteur Antispam « temps réel »

La technologie RPD de Commtouch utilisent des algorithmes d'analyse du trafic mondial (des millions de mails/jour) pour identifier en temps réel des éléments caractéristiques d'un Spam mais indépendants du contenu (par ex : envoi massif de 1 vers N).

- Indépendance vis-à-vis des technologies « classiques » (bayésien, heuristique…..) donc **pas de problématique de mise à jour** et détection de **tout type de contenu** (y compris le spam « Image » ou « musical »)
- **Impact très faible** sur la performance globale
- Un taux de détection parmi les meilleurs du marché **(+ de 95%)** pour un taux de faux-positifs quasi nul **(< à 0,0001%)**