

**La Technologie d'Analyse Répartie du Spam  
In-The-Cloud par NETGEAR® :**

**La Protection réseau contre les menaces  
véhiculées par e-mail**

Ces dernières années, l'e-mail est devenu le vecteur de propagation privilégié de toute une variété de menaces informatiques comme le spam, les virus, les chevaux de Troie et les attaques de phishing (hameçonnage). Comme il est désormais possible d'envoyer des e-mails en masse dans le monde entier, les pirates diffusent en moyenne 40 000 attaques de sécurité chaque jour, soit 15 millions chaque année. Une étude Ferris Research a évalué qu'entre la baisse de productivité et le coût de l'intervention des services d'assistance, le spam avait coûté 35 milliards de dollars aux entreprises américaines en 2007. Au niveau mondial, le coût a atteint 100 milliards de dollars. Selon une étude Nucleus Research, la gestion quotidienne du spam ajoute encore 71 milliards de dollars à la facture réglée par les entreprises américaines.

Cette "réussite" est imputable pour beaucoup au manque d'adaptabilité de la plupart des logiciels de sécurité face à une menace dont la forme évolue constamment. Les créateurs de spam et de malwares utilisent des méthodes de propagation toujours plus subtiles, pour assurer à leurs attaques une diffusion la plus large possible. La majorité des logiciels antispam et autres solutions de sécurité analysent uniquement le courrier entrant, pour y détecter des incohérences dans l'adresse ou l'objet du message. Ce scan effectue uniquement une vérification par comparaison à une liste de règles existantes, et par conséquent, il s'avère incapable de détecter immédiatement la plupart des menaces qui utilisent une technique ou une forme inédite. Pourtant, comme les menaces véhiculées par e-mail sont envoyées à des millions de destinataires quasiment en simultané, il est essentiel de pouvoir les détecter et les bloquer immédiatement pour neutraliser une attaque avec efficacité.

Le Système NETGEAR ProSecure™ STM pour le Management des Menaces Web et E-mail fait appel à la technologie d'analyse répartie du spam in-the-cloud (c'est à dire, via l'Internet) pour collecter en continu des données en provenance de plus de 50 millions de sources différentes dans le monde. Il est capable d'évaluer avec précision et en temps réel la légitimité d'un e-mail en analysant son profil de diffusion plutôt que les informations figurant dans l'objet. Lorsqu'un e-mail est identifié comme étant du spam, le scanner lui attribue une signature et génère immédiatement un fichier profil correspondant. Cette méthode permet de stopper efficacement une attaque avant qu'elle ne se répande trop largement.

L'approche NETGEAR s'appuie sur une constatation : toutes les attaques partagent des caractéristiques communes.

- La plupart des courriers électroniques malveillants ont été modifiés pour qu'il soit difficile de définir des règles de blocage à partir d'une simple analyse de leur contenu. Par exemple, le contenu d'un spam s'affiche souvent sous la forme d'une image, que les filtres de contenu actuels auront du mal à analyser.
- La plupart des attaques s'appuient sur l'envoi de millions de courriers électroniques pour maximiser le taux de réponse possible et garantir à leur initiateur un retour sur investissement maximal
- La plupart des attaques sont diffusées sur un laps de temps très court, qui nécessite la mise en place d'une solution en temps réel pour détecter l'attaque et limiter son impact, voire même l'empêcher
- Les pirates initiateurs de ces attaques déploient des efforts conséquents pour en masquer l'origine, pour qu'il soit difficile de remonter jusqu'à eux

## Le cycle de vie d'une attaque

Les créateurs de malware ont aujourd'hui la possibilité d'envoyer simultanément des e-mails à des millions de destinataires en quelques minutes, grâce aux botnets. Les botnets sont constitués d'un ensemble d'ordinateurs zombies infectés par malware, qui permettent au pirate de contrôler à distance les processus d'un système.

En moyenne, un botnet correspond à un réseau de 20 000 ordinateurs zombies utilisés pour lancer une menace coordonnée à très grande échelle. Les plus grands réseaux de zombies peuvent comporter plus d'un million d'ordinateurs. Lorsque le créateur du malware diffuse une commande, chaque machine infectée présente sur le réseau est activée et diffuse simultanément la commande à distance.

Les virus et autres menaces véhiculés par e-mail se propagent automatiquement dès le moment où ils infectent l'ordinateur d'un utilisateur. Plus le nombre d'ordinateurs infectés à l'origine est important, plus l'attaque sera susceptible d'être diffusée largement. Aussi, il est essentiel de détecter au plus vite le processus d'attaque. En bloquant une attaque dès les premières minutes, on peut contrer efficacement une manœuvre à grande échelle.

### Botnet

Un "bot network", ou "botnet" est un réseau d'ordinateurs infectés par une application logicielle appelée "bot" (robot). Un bot profite généralement d'une faille du système d'exploitation de l'utilisateur ou de l'une des applications installées. En exploitant cette vulnérabilité, le bot peut s'installer automatiquement sur le système, sans aucune action de la part de l'utilisateur. Un bot peut également avoir été installé par un ver ou un cheval de Troie diffusé par un e-mail spammé. Une fois que le bot est installé, l'ordinateur vient grossir les rangs d'un réseau d'ordinateurs infectés, appelés "zombies". Un utilisateur malveillant peut alors le contrôler à distance sans que l'utilisateur légitime de l'ordinateur n'ait donné son autorisation ni même qu'il n'ait conscience de l'intrusion.

### Whaling

Le "whaling" est une forme évoluée de phishing, qui vise les cadres dirigeants d'une entreprise. Le whaling consiste à envoyer un e-mail soigneusement rédigé aux personnes ciblées, pour les inciter à cliquer sur un lien dans le corps du message, qui les dirigera vers un site malveillant d'apparence respectable. Une fois l'utilisateur connecté au site, on peut envoyer un spyware (logiciel espion) sur son ordinateur, ou bien le convaincre de saisir des informations confidentielles personnelles ou concernant l'entreprise. Un exemple classique de whaling aurait la forme d'une facture, d'un courrier des services fiscaux, ou tout autre contenu d'apparence professionnelle.

## Le profil des Messages

Le spam, le phishing et les autres menaces véhiculées par e-mail représentent des millions de messages dont le contenu est volontairement rédigé avec des variantes pour tromper les filtres les plus courants. Cependant, tous les messages faisant partie d'une même attaque partagent au moins une caractéristique spécifique et identifiable, que l'on peut utiliser pour distinguer l'attaque. Souvent, différentes campagnes de spam sont lancées depuis un même réseau d'ordinateurs zombies ; plusieurs vagues de phishing renvoient fréquemment le destinataire vers un même site Internet frauduleux et chaque fois qu'un même virus transporté par e-mail apparaît, il contient toujours le même code malveillant. Même le whaling, la technique de piratage la plus récente, permet de détecter des points communs dans les messages, bien que cette attaque soit très ciblée et diffusée à petite échelle.

Les différents points communs détectés constituent un "profil de message" au sein d'une attaque. Un message qui serait conforme à un ou plusieurs de ces profils spécifiques ferait vraisemblablement partie de l'attaque correspondante.

Le cycle de vie des attaques est généralement assez court, le plus souvent quelques heures à peine. Pour cette raison, une solution de scanning doit impérativement être en mesure de détecter et de classer les messages en temps réel avant que la menace n'ait produit ses effets. En outre, étant donné que la plupart des attaques s'efforcent de dissimuler les messages sous l'apparence d'un e-mail légitime, les solutions qui s'appuient sur une analyse du profil doivent impérativement être capables de faire la distinction entre les communications légitimes et les e-mails frauduleux.

Pour mener de front ces deux objectifs, il faut tout d'abord extraire les profils de message de l'enveloppe des e-mails, de l'objet, et du corps de message sans référence au contenu à proprement parler. On peut appliquer l'analyse de profil pour identifier une attaque quels que soient la langue, le format ou le type de codage du message. Parmi les profils de message, on distingue les profils de diffusion des profils structurels. Par une analyse du mode de diffusion au destinataire, les profils de diffusion permettent de déterminer si le message est légitime ou s'il constitue une menace potentielle, tandis que les profils structurels servent à déterminer l'ampleur de la diffusion.

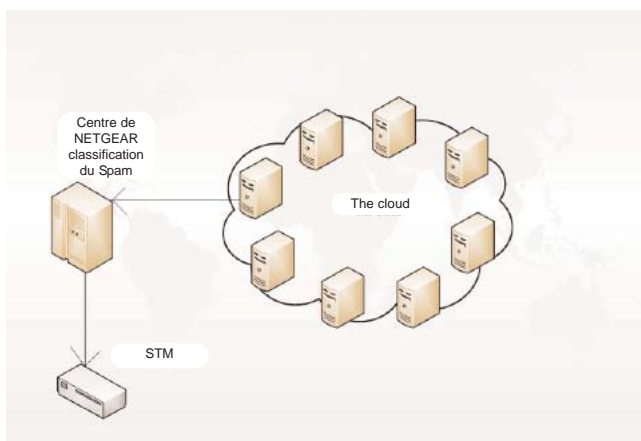


Figure 1: Technologie NETGEAR d'Analyse répartie du spam in-the-cloud

Avec la détection des profils, on a franchi une étape essentielle dans la compréhension du mode de création et de propagation des menaces véhiculées par e-mail. Cette analyse permet à NETGEAR d'identifier de façon proactive et en temps réel les profils nouveaux et spécifiques et de bloquer les nouvelles attaques dès qu'elles sont lancées.

### Technologie NETGEAR d'Analyse répartie du spam in-the-cloud

#### 2: Identifier le Type de Profil.

- " **Bon** " pour les e-mails d'envoi en masse sollicités
- " **Mauvais** " pour les e-mails d'envoi en masse indésirables

#### 4: Catégories enregistrées utilisées pour :

- Détecter le spam
- Détecter les tentatives de phishing.
- Détecter les attaques par un virus nouveau

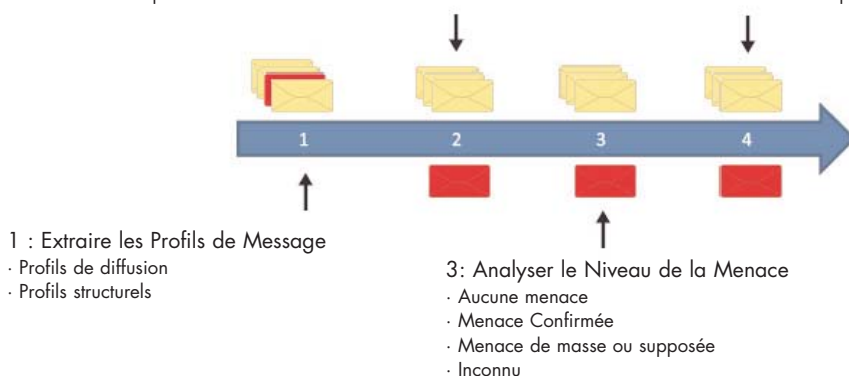


Figure 2: Technologie NETGEAR d'Analyse répartie du spam in-the-cloud

La Technologie NETGEAR d'Analyse répartie du spam in-the-cloud comporte deux éléments : la passerelle Prosecure STM installée sur le réseau de l'entreprise et le Centre NETGEAR de Classification du Spam pour l'Analyse répartie du spam in-the-cloud. Le STM communique avec le Centre de Classification du Spam en temps réel, pour obtenir instantanément des informations sur les attaques de spam et de malware (voir Figure 1).

La communication continue et coordonnée entre les deux systèmes permet à NETGEAR de détecter et classer tous les types de profil de menaces véhiculées par e-mail en temps réel, à partir de l'analyse de données provenant de plus de 50 millions de sources dans le monde. L'Analyse répartie du spam consiste à extraire et à analyser les profils de messages pertinents, puis à les utiliser pour identifier et distinguer les profils de distribution et les profils structurels des attaques propagées par e-mail (voir Figure 2). L'analyse répartie du spam permet d'identifier les nouveaux profils de menaces, mais également d'affiner la catégorisation des profils de messages déjà identifiés.

En effectuant une analyse inversée, le processus d'analyse répartie du spam permet de faire la distinction entre les profils de distribution des envois en masse d'e-mails sollicités, considérés comme une correspondance professionnelle légitime, et les envois en masse d'e-mails indésirables. De cette façon, la technologie d'analyse répartie du spam permet d'identifier la quasi-totalité des messages entrants qui constituent une menace, avec un taux de faux positifs proche de zéro. Elle s'applique à toutes les langues avec une efficacité équivalente quel que soit le format et le type de codage du message.

## Résumé

Pour contrer efficacement les menaces véhiculées par e-mail, les solutions de sécurité doivent désormais relever des défis toujours plus nombreux. L'analyse répartie du spam est une technologie de détection proactive qui ne s'appuie pas uniquement sur le contenu de l'e-mail, et qui permet par conséquent d'identifier un spam dans toutes les langues, quel que soit le format du message, y compris pour les images, les messages HTML et les caractères non rédigés en anglais. L'analyse répartie du spam analyse et classe de façon proactive les nouvelles menaces propagées par e-mail et permet d'établir le profil de l'attaque quelques minutes seulement après son lancement. La technologie d'analyse répartie du spam autorise :

- Un taux élevé de détection du spam, quasiment sans faux positifs
- Une détection très rapide des nouvelles menaces e-mail dès leur apparition
- Une protection contre les tentatives de phishing
- Une protection contre les menaces indifférentes au contenu
- Une protection multilingue contre les menaces
- Une protection multiformats contre les menaces

Grâce à l'analyse avancée des profils, la technologie d'Analyse Répartie du Spam apporte la meilleure protection possible contre les menaces véhiculées par e-mail.

---

## NETGEAR ProSecure STM : Solution de management des menaces Web et E-mail

La passerelle fait appel à une technologie exclusive qui détecte et bloque les attaques de façon appropriée à la rapidité et à l'étendue de leur propagation. Par cette approche, il est possible de détecter le spam et les attaques de malwares dès leur apparition, et de bloquer en temps réel tous les messages associés.

La passerelle intègre la technologie Netgear de Stream Scanning (Scan à la Volée), en attente de brevet, qui permet d'analyser les flux de données au moment où ils entrent sur le réseau. Grâce à la technologie Stream Scanning, les boîtiers NETGEAR STM peuvent traiter un volume important de données en temps réel, une seule analyse suffisant pour identifier le spam, les malwares, les atteintes à la sécurité ou les applications inappropriées. Il est ainsi possible de garantir aux utilisateurs du réseau un contenu e-mail et Web sûr, sans temps d'attente.

La passerelle utilise un système de défense comportemental et proactif qui supprime l'intervalle existant jusqu'alors entre l'exploitation d'une vulnérabilité et sa correction. La solution NETGEAR intègre une analyse chirurgicale qui permet d'identifier les caractéristiques suspectes du trafic réseau entrant et sortant, et de les neutraliser jusqu'à ce qu'elles puissent être examinées de manière approfondie.

NETGEAR, le logo NETGEAR, Connect with Innovation, et ProSecure sont des marques commerciales et/ou déposées de NETGEAR, Inc. et/ou de ses filiales aux États-Unis et/ou dans d'autres pays. Les autres marques mentionnées ici le sont à titre informatif uniquement, et sont susceptibles d'être des marques déposées par leur(s) propriétaire(s) respectif(s). Contenu susceptible d'être modifié sans préavis.  
© 2009 NETGEAR, Inc. Tous droits réservés.