SECTION INTERNET DU CLUB MEDERIC DE MARSEILLE

# Internet Gazette

Site : http://aviquesnel.free.fr/Mederic

**26 mai 2008**

**Numéro 76**

**Sommaire**



## Euro 2008 premières tentatives de piratage

L'Euro 2008 donne des idées aux pirates. Deux semaines avant le coup d'envoi de la compétition, des tentatives d'attaques ont déjà été repérées, pour piéger les fans de football.

Selon l'éditeur d'antivirus G DATA, des messages arrivent dans les boites mails, proposant des places pour les matches, des vidéos censées être exclusives, ou encore des informations telles que les horaires des différentes rencontres. Des offres alléchantes également proposées sur des sites.

Les pages contenant ces éléments dissimulent du code malveillant. Si l'utilisateur clique, il l'installe sur son système à son insu. Le but, pour les pirates est double : récupérer les données personnelles et confidentielles stockées sur la machine, et intégrer cette dernière à un réseau de PC zombies (botnet), utilisé pour l'envoi de campagnes massives de spam.

G Data s'attend à comptabiliser de nombreuses victimes étant donné l'envergure de l'événement. L'éditeur recommande de mettre à jour les antivirus, de désactiver JavaScript dans le navigateur et de supprimer les courriers électroniques non sollicités sans cliquer sur les liens intégrés.

## Lutte anti-piratage : où en est-on sur le plan technique ?

*Le directeur d'Advestigo, Marc Michel Pic a bien voulu répondre à nos questions. Sa société vient tout juste de fournir à la Gendarmerie nationale sa solution AdvestiSEARCH pour être épaulée dans la lutte contre la criminalité en ligne.*

*Outre une présentation de ce système, sont également abordés les thèmes sensibles de la surveillance des réseaux P2P et donc de la Mission Olivennes, la société étant l'un des acteurs les plus connus de ce secteur promu à un riche avenir.*

***Pouvez-vous nous présenter la solution AdvestiSEARCH qui a été choisie par la Gendarmerie ?***

*C'est un outil de surveillance de contenu web, du moins dans le cas de la gendarmerie, qui a pour vocation de reconnaître des contenus par similarités : les gendarmes posent comme question des images ou du texte de référence (des descriptions de fabrication de bombe, des photos pédopornographiques, etc.) et le système va fouiller à partir d'un certain nombre d'informations complémentaires sur d'autres moteurs de recherches, des sites de blogs, des endroits cibles paramétrés par les utilisateurs. Il va alors explorer et récupérer*

*les contenus suspects ou qui potentiellement peuvent avoir un rapport. Il calcule dessus une empreinte pour la comparer avec la base de référence des documents émis par les utilisateurs. En cas de match, l'outil présente l'endroit, la date, l'heure et le comparatif.*

***Les algorithmes fonctionnent comme un moteur de recherche ?***

*Pas exactement. Le moteur de recherche indexe et fouille tout dans une énorme base pour venir répondre aux questions des utilisateurs. Là, la démarche se fait dans l'autre sens. C'est une démarche « spider » sur ce que l'on sait être intéressant : on vient poser des questions à différents moteurs de recherche, un peu à la manière de Copernic. Sauf que la fouille est plus complexe car on peut explorer les sites, leurs ramifications, on peut remplir des formulaires, se mettre dans des pages orphelines qui n'ont pas de lien direct, mais une dénomination URL similaire à une autre existante, bref toutes les stratégies pour créer du web parallèle, le web invisible.*

*On va alors récupérer les endroits intéressants par la dénomination textuelle. On y récupère les textes (Word, PDF, etc.) ou les images (sous différents formats). On vient les aspirer pour calculer nos empreintes dessus et même reconnaitre des variations des textes ou des images : une image mise sur ces sites et transformée (recompressée, découpée, présentée en extrait) ou un texte utilisant des synonymes, ou découpé, plagié, etc. seront reconnus.*

***On est là dans une vision où un utilisateur interroge un réseau depuis un poste local. Peut-on envisager un tel système de surveillance aux nœuds du réseau ?***

*On va là au-delà du produit « SEARCH » mais l'idée est envisageable. Notre solution existe pour le texte, l'image, la vidéo et le son. On s'en sert aujourd'hui pour faire de la surveillance opérée par nos services pour les ayants droit ; nous surveillons par exemple des sites comme Youtube ou Dailymotion de manière à retrouver des contenus qui sont plagiaires (séries, TV , émissions, films). Nous faisons cela de manière externe à ces sites. Notre client est averti de l'existence d'un contenu à problème et il prend les mesures pour faire retirer les contenus.*

*De la même manière, AdvestiSEARCH dans sa version P2P est à la base de notre offre de mise en œuvre de la 'Réponse Graduée' préconisée à très court terme par les accords Olivennes.' Ce déploiement externe peut également être interne du côté des opérateurs. Mais le problème est la volumétrie qui n'a rien à voir.*

*Deux cas de figure. Pour le cas du P2P, il y a des solutions parce que les protocoles reposent structurellement sur des hashs, les résumés des fichiers. Le principe de fonctionnement du P2P repose sur des tables de hash distribuées. Ces hashs peuvent être utilisés en amont, pour repérer les fichiers qui sont copyrightés, en aval, pour dire que tous les hashs de ce type-là vont être blacklistés par un module chez l'opérateur. C'est techniquement faisable même dans des contextes de grande bande passante opérateur (10 Gbits). Nous avons d'ailleurs fait des démonstrations récentes avec une société partenaire spécialisée dans ces outils là pour le compte d'ayants droit audio, vidéo.*

***C'est typiquement les tests préconisés par la mission Olivennes, non ?***

*Ce sont des produits qui peuvent exactement rentrer dans le cadre de ces tests.*

***Ces tests Olivennes ont-ils commencé ?***

*Les tests sont prévus dans les deux ans, on s'attend plutôt à ce que ce soit pour la deuxième année.*

***Les majors sont très pressées...***

*Oui, mais les FAI moins ! (rire) Et il n'y a pas encore de calendrier de tels tests ; par contre, le premier volet de 'Réponse Graduée', basé sur une observation externe des échanges, devrait être mis en œuvre très rapidement. Il fait, lui, l'unanimité et le principe semble en être rapidement repris à l'étranger (UK, Japon, Australie par exemple).*

*Aujourd'hui, nous ne vendons pas ce type de produit réseau, mais nous travaillons avec deux sociétés qui développent ces solutions. Ce sont des technologies assez différentes d'Advestigo. Nous, ce que nous proposons, c'est la constitution*

*des bases de hashs validées qui servent à identifier ces contenus.*

*À l'échelle des réseaux, il y a différents problèmes qui peuvent survenir d'ici là, dont les mécanismes de cryptage qui vont agir contre ces produits. Mais ces produits ont des réponses. Si on doit compter une année pour la mise en place des tests, il faudra bien évaluer la situation dans un an par rapport aux technologies effectives sur les réseaux.*

***Le comité des ministres du Conseil de l'Europe a adopté plusieurs recommandations en matière de filtrage. Une première réaction ?***

*Les choses ne sont pas encore stabilisées. Elles devraient évoluer dans les deux ans. Dans un premier temps, il y a un schéma d'expérimentation qui doit être mis en place. On devrait avoir pas mal de valses-hésitations.*

***Pour en revenir à ces questions de chiffrage, ce n'est pas une guerre perdue d'avance ?***

*Rappelons d'abord que le problème du cryptage ne se pose pas dans le cas de la Réponse Graduée. [NDLR : ce système de surveillance se positionne comme client usuel du protocole].*

*Le problème pour les systèmes de filtrage réseau est le suivant : si en France se met en place unilatéralement un mécanisme de ce type et que les internautes disons Américains ne voient aucune raison de s'embêter avec un mécanisme crypté, alors il sera nécessaire, pour que le P2P continue à être efficace, qu'apparaissent des mécanismes pour faire le lien entre un univers crypté et un univers non crypté facilement. Et ce, sans apparition d'un inconvénient pour les utilisateurs qui ne sont pas concernés. Alors peut-être que cela pourra effectivement permettre un cryptage à grande échelle en France, mais ce n'est tout de même pas gagné d'avance.*

*Le problème du P2P est qu'il est un problème mondial. Si on met en place une solution qui protège les échangeurs de contenus en France, cela veut dire qu'il n'y aura que des contenus intéressants et français sur ces réseaux-là, et que la source de contenus externes aura du mal à arriver. Ce qui est un peu à contresens de ce qui se passe sur les réseaux aujourd'hui saturés de productions anglo-saxonnes.*

*Là-dessus, il faut vraiment voir : le cryptage est une difficulté claire en particulier en termes de puissance. Il y a des réponses légales. Mon estimation actuelle est que d'ici un an il n'y aura pas de basculement au cryptage important. Au-delà, l'évolution des gens vers de véritables réseaux cryptés prendra du temps. Et je parle de véritable système de cryptage, pas ceux qui sont pseudo cryptés, sans distribution de clefs protégées. Vous avez pas mal de systèmes sur Bittorent, edonkey avec échange de clef préalable et donc interceptables.*

***J'avais plutôt en tête Freenet** Oui, voilà ou Mute, des réseaux qui sont plus sérieux. Maintenant il faut voir s'ils arrivent à remplacer les réseaux actuels. Le facteur de migration est extrêmement difficile à maitriser.*

***Difficile peut-être pour monsieur Tout-le-Monde de passer sous Freenet...***

*On peut imaginer qu'un produit simplifie tout cela ; en regardant comment se sont déployés des produits comme PGP, on peut imaginer que des infrastructures de diffusion de clefs publiques se mettent en place. Mais d'un autre côté, quand on voit à quel point il est difficile dans une entreprise de déployer ce type de solution, on se dit que ce n'est pas gagné pour le P2P.*

## *Un magnétoscope gratuit débarque sur la Toile*

**Avec Wizzgo.com** , les magnétoscopes risquent de prendre un petit coup de vieux en plus. Créé par Philippe Savary, ancien financier reconverti dans la production cinéma et audiovisuelle, et Jérôme Taillé-Rousseau, ancien conseiller de la ministre de la Culture et de la Communication entre 2000 et 2002, ce site permet aux internautes de choisir, de télécharger et de visionner gratuitement 4 Go de programmes télévisés par mois. La seule condition ? Opter pour un programme diffusé sur l'une des 17 chaînes de la télévision numérique terrestre (TNT).

Pour enregistrer, le mode d'emploi est simple. L'utilisateur télécharge le logiciel compatible Mac et PC via le site wizzgo.com, s'inscrit pour recevoir un identifiant et commande le programme désiré en un clic. Pour que la commande soit possible, il faut par contre que l'internaute choisisse son programme au plus tôt 14 jours en amont et au plus tard dans les cinq minutes qui précèdent la diffusion.

Une fois le programme enregistré, l'utilisateur reçoit une copie cryptée et personnalisée à visionner sur son ordinateur ou son iPod. Compte tenu qu'un Français sur deux préfère regarder la télévision en différé, wizzgo.com espère surfer sur ce créneau pour enterrer un peu plus le format VHS... Avec en toile de fond, le souhait que la publicité présente sur le site Internet suffise à financer ce concept pour le moins innovant.

## *L'opérateur Orange réplique aux services de Free, Neuf ou encore Alice*

*Orange a comblé en très peu de temps le vide qui le séparait de ses concurrents. L'opérateur s'apprête à lancer un service de stockage de données en ligne. Baptisé "**mes données**", le nouvel outil, accessible depuis n'importe quel poste, offre aux utilisateurs la possibilité de stocker des données sur un espace compris entre **2** et **4 Go**.*

*L'espace de stockage peut aussi bien accueillir des matériaux ludiques (vidéo, photos, musiques) que professionnels (document Word ou Powerpoint).*

*Le service, **gratuit**, est uniquement réservé aux abonnés Orange. Seuls les clients détenteurs d'un forfait mobile et d'un abonnement Internet, et ayant activé l'option "mes services unifiés" pourront bénéficier des 4 Go de stockage. Les autres devront se contenter des 2 Go.*

*A partir d'août, les clients d'Orange pourront profiter de 10 Go de stockage en souscrivant à une option premium facturée 3 euros par mois.*

*Orange semble avoir particulièrement insisté sur l'interface utilisateur. L'outil, accessible depuis la page d'accueil Orange, est supposé être très maniable et intuitif. Selon le communiqué, un simple 'glisser-déposer' permet d'intégrer un contenu dans l'espace de stockage. En outre, grâce à une application supplémentaire installée sur PC, l'espace de stockage peut arborer la forme d'un disque dur externe et se comporter comme tel.*

*Pour se démarquer, Orange joue la carte de la convergence. Lié avec d'autres services proposés par l'opérateur, l'utilisateur peut par exemple gérer ses photos avec le service Photo Orange. Parmi d'autres innovations prévues, une future évolution de l'outil doit permettre de copier directement sur son espace de stockage des contenus issus d'un mail.*

*Rappelons toutefois qu'Orange n'est pas seul dans ce domaine. Depuis 2005, Neuf propose à ses abonnées le service 'Neuf Giga. Avec ce service, les utilisateurs peuvent stocker **jusqu'à 9 Go de données**. Selon* Neteco*, la très convoitée Alice lance également son service de stockage en ligne. Moyennant **5 euros par mois**, son offre, 'Alice back up', permet à ses abonnés de disposer d'un espace de stockage en ligne. Contrairement, aux offres précédentes, Alice ne fixe aucune limite de stockage assez conséquent, mais n'autorise ni la consultation en ligne, ni le partage de fichier.*