

MARC BLANCHARD VIRUS DOCTEUR

[Définition&Explications] Le SPAM

On parle du spam, de courriers indésirables, de publicités non-sollicité, etc... ces messages qui nous envahissent chaque jour.

Essayons de comprendre les processus et les concepts de ces messages qui nous font perdre un temps fou !

Définition :

Un spam est un message que le créateur souhaite faire passer sur un ou plusieurs supports électroniques :

- mail,
- web,
- messageries instantanées,
- SMS,
- MMS,
- etc..

Les contenus sont divers:

- Produits frelatés ou expirés
- Produits illégaux
- Contrefaçons ou copies de mauvaise qualité
- Messages politiques et financiers
- Vols ou escroqueries de biens ou cartes de crédits
- Messages pornographiques
- Chaines de vie ou de mort

- Un service particulièrement nouveau ou un mensonge

Le temps perdu :

Le cerveau humain travaille en parallèle : nous lisons, nous pensons parfois à autre chose pendant que nous écoutons mais restons attentif, nous respirons, bref tous ces sens font travailler notre cerveau en parallèle.

Mais revenons à notre fonctionnement intellectuel face à notre outils favori : Le courrier électronique :-)

Pour déterminer, interpréter et effectuer une action sur un message reçu, il ne faut pas moins de 2,5 sec, car dans ce cas, le cerveau fonctionne en série. Il travaille en série, car c'est notre logiciel de courrier électronique qui ne nous permet pas de travailler en parallèle. En fait, nous lisons chaque message électronique, les uns après les autres !!! Donc notre cerveau travaille en série !

Pourquoi les mêmes spams nous arrivent malgré des filtrages ?

Le SPAM est :

- Une volonté
- Une création avec logiques humaines
- Une action
- Une analyse des résultats obtenus

Si les conditions de blocage de spam sont « matchées » c'est à dire que les spams sont arrêtés par un logiciel AntiSpam, alors le spammeur fera en sorte d'y effectuer des modifications jusqu'à ne plus être arrêté.

Pour comprendre les réflexions des spammeurs, ou même des créateurs de virus, il faut connaître 3 types d'analyses d'interprétation que le cerveau humain peut effectuer :

- Schématisation d'un système connu
- Schématisation Isomorphique
- Schématisation Homomorphique

Ce qui aura pour résultante un même résultat mais utilisant une technique différente utilisant alors un système d'Influences.

Mesure de l'information : étude de cas

Supposons que nous recevons un spam de ce type : « Le produit YYY, c'est bon pour toi »

Suivi d'une url du type :

« www.yyy.com/offer/discount.html »

Fonctionnement inconscient de notre cerveau :

« Le produit YYY » : représente une curiosité car il s'agit d'un nouveau produit

« c'est bon » : représente une préconisation

« pour toi » : est une influence personnelle

Par conséquent, la victime ressent un sentiment de CURIOSITE, car :

- on prend soin de la victime

- la victime est déjà en confiance avec ce slogan

Donc : la victime est sur le point de visiter le site !

Mais, le spammeur remet une couche d'influence pour finaliser l'autovolonté de la victime et lui montrer qu'il faut absolument cliquer sur le lien !

« www.yyy.com/offer/discount.html »

Chacun d'entre-nous savons ce qu'est un discount ! Une offre exceptionnelle !!

Par conséquent, la victime est quasiment persuadée qu'elle ira faire une bonne affaire ...en cliquant sur le lien !!!

Définition : schématisation d'un système connu :

Une interprétation peut être effectuée sous plusieurs formes :

- Analyse sous forme de dictionnaire dans un cadre conceptuel par rapport à la schématisation d'un système connu, avec ou sans variables, avec ou sans espace de phase en 3D

Définition : schématisation isomorphique :

Peut être considérée comme isomorphe un système pouvant subir une seule variation de transformation à un objet soumis et connu.

Dans notre exemple : « c'est bon »

Définition : schématisation homomorphique :

Une suite d'au moins deux analyses isomorphiques et pouvant faire intervenir des objets extérieurs en faisant des probabilités de séquences et/ou des influences.

Dans notre exemple : « c'est bon » ET « pour toi »

Définition : Les Influences :

Analyse dite Analyse d'Univers de Phase qui peut être provoquée par :

- Une influence externe,
- Une influence connue ou réconfortante
- Et/ou lorsque un objet change d'état,

Dans notre exemple : « www.yyy.com/offer/discount.html »

Résultat :

Remise en cause de l'influence de départ que l'on souhaiterait obtenir comme résultat, mais on s'y force si l'on souhaite quelque chose avec conviction.

En conclusion : Les systèmes d'influences

Ainsi, si on veut établir une mesure de l'information, on doit tenir compte du degré d'incertitude lié à chaque cas possible.

Mais on peut en déduire alors la volonté de la victime pour acquérir le produit : pour cela, le spammeur veillera à le conforter une fois de plus en s'appuyant sur les mêmes techniques que ci-dessus en ayant pris soin de renforcer le système d'influence sur le site web « www.yyy.com/offer/discount.html » en communiquant sur :

- Les facilités de paiements
- Les délais de livraison
- Les garanties (satisfait/remboursé)
- Les promotions exceptionnelles voire gratuite
- Des couleurs et des logos de couleurs chaudes, des gens sur les photos souriantes, etc?

Spam : Techniquement : Les envois :

L'annonceur et le spammeur peuvent être la même personne et/ou la même société.

Les techniques d'acheminement du mail peuvent se faire :

- En exploitant les failles de relay des serveurs de messageries
- En exploitant des failles Mail via des proxy http
- En installant une porte dérobée (backdoor) de micro serveur SMTP sur les postes zombies des

victimes ayant reçu le spam et ayant visité leurs sites

- En transformant, dans ce cas, le poste de la victime en serveur de spam ou de serveur web du spammeur. Dans ce cas, la machine victime devient une machine zombie dont l'utilisateur n'est pas le seul utilisateur de sa propre machine. Sa machine devient alors une machine prête à lancer une attaque télécommandée sur des sites commerciaux et/ou professionnels, et peut ainsi aider un hacker à faire du chantage, ou pire encore, devenir une machine serveur hébergeant des photos très compromettantes...

Mais comment ont-ils mon adresse mail ?

Les spammeurs utilisent des techniques diverses:

- Rachat de mailing listes
- Crawler (sniffeurs) SMTP sous forme de backdoor (tout courrier électronique est échantillonné et envoyé au spammer, pris sur les blogs, forums, carnet d'adresses, etc)
- Echange d'adresses : sur les undergrounds
- Spam de vente d'adresses mail qui sont générés uniquement pour obtenir votre mail
- Les réponses aux spams par « désabonnement »
- Les syphonages de sites web récapitulant les discussions des news-groups
- Des syphonages de pages HTML contenant des adresses mails
- Des vers syphonant des mails locaux et les WAB ou les carnets d'adresses de leurs victimes
- Technique de génération de mails automatiques par dictionnaires croisés !

Cette technique est utilisée pour un spam des utilisateurs de grands FAIs (fournisseurs d'accès internet) :

- Dictionnaire de noms / pays (ex: Smith) , les plus populaires du pays à spammer
- Dictionnaire de prénoms / pays (Paul, Brian, etc) , les plus populaires du pays à spammer
- Dictionnaire des noms des FAIs (aol.com)

Résultats de ces robots :

- Paul.smith@aol.com
- Smith.paul@aol.com
- Paulsmith@aol.com
- Paul1smith@aol.com

- Paul_smith@aol.com

- Etc?

Donc les tentatives seront effectuées les unes après les autres sur ces adresses. Lorsqu'il n'y aura plus d'erreur de la part du serveur de courriers destinataires, le pirate pourra être certain que cette adresse mail est correcte, et il en essaiera d'autres avec d'autres noms et prénoms...et ainsi de suite...

Conclusion :

Le spam n'est pas une suite de numérique facilement détectable, car comme vous l'avez certainement compris, les spammeurs utilisent des techniques évolutives, dont les contenus changent très régulièrement, comme par exemple : envoyer le contenu du spam dans une image ou un document acrobat en PDF, etc...

C'est pourquoi qu'un antispam doit pouvoir analyser les courriers électroniques avec de nombreuses technologies de détections associées à des filtrages linguistiques, listes de serveurs de mails déclarés en listes noires ou en relais ouverts.

Aujourd'hui, selon spamhaus.org, la France est au 9eme rang mondial des relais de serveurs propageant du spamC'est à réfléchir....

...et surtout, à s'équiper si on ne veut pas perdre du temps à lire des informations inutile, et à être productif dans un système travaillant en série (je veux dire le courrier électronique :-)

Commentaires

2007-09-26 02:52:04 - Sergey -
<http://grandpublic.kaspersky.fr/forum/viewtopic.php?p=51900#51900>

Que dire, mis a part merci, clair, net accessible a tous :-)

2007-09-27 11:10:36 - Jean 32

Effectivement : merci ! Mais que peut faire de plus le novice en ayant déjà KIS 7.0.0.125, m'aj chaque heure, pour être à l'abri ?

Formidable idée de Thierry de faire connaître ces infos de Marc, merci à tous.

2007-10-02 11:09:39 - Découragée

bonjour, c'est vraiment intéressant, mais ne m'aide pas . Un éditeur non sollicité qui m'est inconnu m'envoie chaque jour un épisode d'un feuilleton qui en comporte 202 ! Je me suis désabonnée plusieurs fois alors que je ne m'étais jamais abonnée, mais CA CONTINUE et je ne sais plus que faire. Il s'agit de P.O.L.Editeurs, feuilleton "la république de Mek Ouyes V" . Ce matin il m'est parvenu dans "courrier indésirable", et l'explication donnée : probable tentative de phishing ou hameçonnage . Que faire de SIMPLE pour m'en débarrasser définitivement ? Je suis totalement novice en informatique! Merci de bien vouloir me répondre.,

2007-10-03 00:23:28 - Marc Blanchard [Virus Docteur] - marc.blanchard@fr.kaspersky.com

Bonjour Découragée, Déjà si le message est entré dans le dossier indésirable, cela signifie que ce courrier est classifié en tant que spam ou effectivement phishing/pharming. Je me permettrai une petite remarque, vous continuez de recevoir des courriers de ce type, car vous avez cherché à vous désabonner en cliquant sur le lien. Vous n'avez fait, en fait, que de confirmer l'existence de votre adresse mail. Le problème est que maintenant, vous allez recevoir de nombreux spams car les cyber-délinquants se redistribuent les adresses de courriers électroniques existantes. Pas de panique, des outils de sécurité comme des antispam associés à des suites antivirus dit internet security suite vous apportent des solutions tels que controle parental, antispam, antiphishing, protection des envois de données confidentielles tels que mots de passes de sites sécurisés, etc... Travaillant chez Kaspersky, je ne peux que vous conseiller notre suite de sécurité KIS qui comporte tout un panel d'options de sécurités qui vous aideront à rester protégé efficacement. N'étant pas commercial, je vous donne deux liens qui vous renseigneront d'avantages: Le forum des utilisateurs : <http://grandpublic.kaspersky.fr/forum/> L'achat en ligne : <http://kaspersky.telechargement.fr/>

Copyright : Blanchard [Virus Docteur] Marc - 2007-09-25 19:11:07
Creative Commons Deed

Paternité - Pas d'Utilisation Commerciale - Pas de Modification 2.5

Vous êtes libres :

- * de reproduire, distribuer et communiquer cette création au public

Selon les conditions suivantes :

Paternité. Vous devez citer le nom de l'auteur original.

Pas d'Utilisation Commerciale. Vous n'avez pas le droit d'utiliser cette création à des fins commerciales.

Pas de Modification. Vous n'avez pas le droit de modifier, de transformer ou d'adapter cette création.

* A chaque réutilisation ou distribution, vous devez faire apparaître clairement aux autres les conditions contractuelles de mise à disposition de cette création.

* Chacune de ces conditions peut être levée si vous obtenez l'autorisation du titulaire des droits.

Ce qui précède n'affecte en rien vos droits en tant qu'utilisateur (exceptions au droit d'auteur : copies réservées à l'usage privé du copiste, courtes citations, parodie...)

Ceci est le Résumé Explicatif du Code Juridique (la version intégrale du contrat).

<http://creativecommons.org/licenses/by-nc-nd/2.5/>