

Le top des attaques Internet 2009



Photos by PR Photos

Quelles ont été les 5 célébrités les plus dangereuses en 2009?

Les spammeurs savent-ils vraiment qui a tué Michael Jackson?

Le top 5 des célébrités toxiques en 2009



Michael Jackson – La mort du Roi de la Pop a généré un déluge d'envoi de spam et de maliciels juste quelques heures après son décès, le 25 juin 2009. Les cybercriminels savaient bien que la mort du chanteur intéresserait le plus grand nombre de personnes, que cette actualité serait un moyen idéal de capter l'attention des internautes, et ainsi d'augmenter l'ouverture d'emails frauduleux ou de pousser à cliquer sur des liens nuisibles.

Serena Williams – L'esclandre de la star du tennis pendant l'US Open 2009 a généré de nombreuses pages vues sur Internet. A partir du moment où c'est devenu une des vidéos les plus recherchées, les cybercriminels ont infiltré des sites web en prétendant qu'ils avaient la vidéo et en y intégrant de faux antivirus appelés « facticiels ».



Patrick Swayze – Comme pour le décès de Michael Jackson, les cybercriminels ont profité des recherches faites sur de la disparition de Patrick Swayze pour diffuser des maliciels, notamment hébergés sur des sites web compromis.

Harry Potter – A l'occasion de la sortie du 6^{ème} volet de la saga Harry Potter au cinéma, Les spammers et les scammers ont profité de l'engouement pour envoyer un grand nombre de spams avec « Harry Potter » dans l'objet du message. Les fans à la recherche d'une bande annonce ont ainsi été redirigés vers une série de sites hébergeant des maliciels.



Président Barack Obama – Non seulement le 44^{ème} Président des États-Unis a été élu par les Américains, mais il a également gagné les suffrages des cybercriminels qui se sont servis de son nom et de certains points clés de son programme tels que la réforme du système de santé ou la relance de l'économie pour diffuser des maliciels et des spams.

Le Top des menaces & des actus Internet de 2009



Conficker

Découvert en novembre 2008, Conficker a fait beaucoup de bruit en mars et avril dernier. Ce vers permet entre autre à ses créateurs d'installer à distance des maliciels sur les machines infectées. L'impact causé par ce maliciel est encore difficile à estimer à ce jour.

Une attaque de déni de service répandu par W32.Dozer

W32.Dozer a commencé à se répandre le 4 juillet 2009, entraînant une attaque en déni de service contre des sites gouvernementaux, financiers et médias, aux États-Unis et en Corée du Sud.



Opération Phish Phry

En Octobre 2009, le FBI a lancé l'opération "Phish Phry," et démantelé un réseau de vol d'identité qui avait fait plusieurs milliers de victimes. Selon le FBI, c'était le plus gros réseau de cybercriminels découvert à ce jour.

Les faux logiciels Antivirus ou "Facticiels"

Les facticiels, piègent les consommateurs et les incitent à télécharger des applications, souvent à partir de sites peu connus. Les scammers s'appuient sur des messages alarmistes et d'autres tactiques d'ingénierie sociale, pour duper les internautes et leur faire acheter et installer de faux antivirus.



Albert Gonzalez

En août 2009, les autorités américaines ont annoncé la mise en examen de plusieurs personnes, dont Albert Gonzales, les accusant d'avoir été à l'origine des plus grandes fuites de données de ces dernières années.



Le top “objets” de spam en 2009

Saviez-vous que Symantec a vu passer plus de 40 trillions de spams au cours des 12 derniers mois? C’est plus de 5000 spams par personne dans le monde aujourd’hui ! Voici quelques-uns des plus grands succès mondiaux des spammeurs en 2009.

“Devez-vous de l’argent aux Impôts?”

Il faut l’admettre, personne n’aime payer ses impôts. Les spammeurs l’ont bien compris et en profitent en essayant de faire croire à tout un chacun qu’ils ont les moyens de les en dispenser.

“Inscrivez-vous à notre séminaire Halloween, pour des soirées, des citrouilles, de la décoration et plus encore!”

Choisissez une fête, n’importe laquelle et vous pouvez être sûr que vous trouverez des spams à son sujet. De Noël au Nouvel An Chinois c’est tous les jours la fête pour les spammeurs.

“Pas de mutuelle, et pas les moyens d’acheter des médicaments? Vous pouvez maintenant grâce au programme médical sponsorisé par Obama”

Voici une double arnaque pour vous faire ouvrir l’email, utilisant deux des sujets les plus populaires en 2009 : Obama, et le programme de santé aux États-Unis.

“Qui a tué Michael Jackson?”

Un des sujets les plus demandés au moment du décès de MJ. Les spammeurs en ont profité pour infester l’internet avec des spams « révélant » qui avait tué MJ ou même qu’il était encore en vie (Tout comme le sont encore Elvis et Tupac...)



Le top “objets” de spam en 2009

“L’édition complète d’Harry Potter sur Ebook”

Les spammers ont profité de la Harry Pottermania lors de la sortie de “Harry Potter et le prince de sang-mêlé” cet été. Est-ce que Twilight sera également sur leur liste?

“Vos amis vous invitent sur twitter!”

Même les spammers profitent de l’engouement pour Twitter en envoyant des messages qui prétendent être une invitation Twitter. Symantec a également vu des spams publicitaires sur comment gagner de l’argent via Twitter.

“Offre de votre concessionnaire : réduction de 35% sur l’achat de votre nouvelle voiture”

De la réduction aux offres de paiements lors de l’achat de nouvelles voitures, les spammeurs s’intéressent aussi à la situation économique... Car ils savent que cela vous intéresse. La situation économique étant une thématique à la mode, les spammeurs savent qu’ils pourront en récolter quelques fruits.

“Pour un meilleur travail, obtenez un diplôme”

La publicité pour obtenir de nouveaux diplômes est une arnaque classique des spammeurs.

“Trouvez vos médicaments contre la grippe H1N1 ici”

Qui veut attendre des heures pour se faire vacciner contre la grippe H1N1? Quand il suffit seulement d’ouvrir un email ou de cliquer sur un lien pour bénéficier des derniers scoops des spammeurs sur comment se protéger efficacement.

“N’allez pas faire d’hypothèques”

Avec la crise économique, le nombre d’hypothèques a explosé, rendant ce sujet très populaire pour les spammeurs.

Quelles menaces pour 2010?

- **Savez-vous qui sont réellement vos amis?** – La popularité des réseaux sociaux ne fera que s'accroître en 2010, ce qui risque d'entraîner un nombre croissant de fraudes sur ces mêmes sites.
- **Les vendeurs de maliciels vont s'améliorer** – En 2010, attendez-vous à voir les vendeurs de facticiels (faux antivirus) améliorer leurs techniques, y compris en détournant des ordinateurs, les rendant inutilisables, et en les « rendant » aux propriétaires seulement après paiement d'une rançon.
- **Augmentation des maliciels sur MAC et Smartphones** – Tandis que la popularité et les parts de marché des MAC et des Smartphones vont augmenter en 2010, les cybercriminels vont passer plus de temps à développer des menaces dédiées à ces outils.
- **Attention à vos tweets** – Les adresses URL raccourcies sont courantes sur Twitter et autres sites de réseaux sociaux. Étant donné que l'on sait rarement ce qui se cache derrière une adresse URL raccourcie, les attaques de phishing peuvent ainsi être dissimulées et conduire les internautes sur des sites compromis.
- **La Cyber-Intelligence** – De plus en plus de cybercriminels s'attaquent directement à VOUS en vous forçant à télécharger des maliciels. Vous pensez télécharger un logiciel légitime, mais non. Vous pouvez ainsi ouvrir les portes à un vol d'identité ou d'autres menaces cybercriminelles. Symantec estime que le nombre d'attaques utilisant l'ingénierie sociale va augmenter considérablement en 2010.

Préparez-vous, Protégez-vous

- N'ouvrez jamais **des emails suspects ou des pièces jointes de personnes que vous ne connaissez pas**.
- Ne répondez pas **aux emails qui vous demandent des informations personnelles**.
- **Utilisez une suite de sécurité à jour**, achetée chez un vendeur reconnu, par le biais d'un réseau de distribution connu.
- Quand on vous propose d'accepter ou de refuser la connexion d'une application à internet, **refusez toujours, sauf si vous êtes sûr**, que le site sur lequel vous vous connectez est authentique et sécurisé.
- Si vous êtes connecté sur **un réseau WIFI, sécurisez le avec un mot de passe**, et n'autorisez pas d'autres ordinateurs à se connecter à votre réseau privé.
- Utilisez des **phrases de passe**. Changez en régulièrement, et n'utilisez pas les mêmes pour tous vos sites.
- **Ne donnez pas vos coordonnées bancaires à des sites qui ne sont pas de confiance**. Vérifiez qu'ils ont bien « https:// » au début de leur adresse **internet**, et que le cadenas fermé est bien présent en bas à droite de votre écran.
- **Utilisez un service de réputation des sites web**, qui peut vous prévenir à l'avance si le site sur lequel vous vous connectez est ou n'est pas compromis.
- **Regardez vos relevés bancaires et vos relevés de cartes de crédit régulièrement**, et recherchez les transactions douteuses.
- Pour plus d'information sur le marché de la cybercriminalité et les moyens de se protéger, rendez-vous sur **www.chaqueclicompte.fr**



Photos by PR Photos

Norton[™]
from symantec