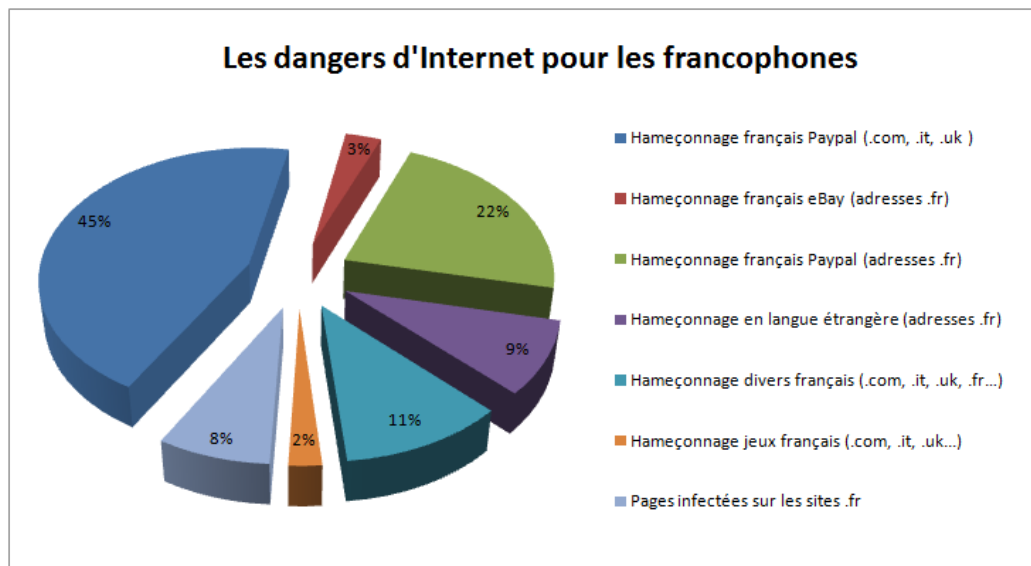




Les dangers du Web pour l'internaute francophone

Pour répandre leurs malwares et leurs fausses pages d'hameçonnage, les cybercriminels se reposent sur la puissance de la toile. Des milliers de nouvelles pages Internet apparaissent chaque jour dans le monde pour véhiculer virus et escroqueries. Quel risque pour l'internaute francophone ?

Beaucoup d'internautes francophone surfent exclusivement sur des sites en français et mettent automatiquement à la corbeille tous les courriels qu'ils reçoivent en langues étrangères. Pour définir quel risque réel prend ce type d'internaute lorsqu'il navigue sur Internet et reçoit des courriels, G Data Software a mené trois mois d'étude. À l'aide de ses outils de collectes, l'éditeur a recensé les pages Internet dangereuses en langue française ou comportant dans leurs adresses l'extension .fr. Il livre ici les résultats et leur analyse.



Étude réalisée entre le 1^{er} janvier et le 31 mars 2010 sur un échantillon représentatif de 1000 pages Internet en français et/ou comportant dans leurs liens l'extension .fr. La collecte et l'analyse des pages relevées sont réalisées à l'aide des systèmes G Data Software AG.

Les sites perso français mal protégés

Un des premiers points à relever de cette étude est le nombre croissant de sites Internet français hébergeant de l'hameçonnage et des malwares. 42 % des pages collectées sont liées à un site existant de langue française (adresses .fr). Il s'agit pour la plupart de sites de particuliers, d'association, de club sportif ou de petites entreprises. Gérés par des administrateurs non spécialisés, ces sites sont souvent mal sécurisés et représentent un terrain productif où les cybercriminels viennent semer leurs méfaits.

L'hameçonnage français prend de l'ampleur

Du côté des typologies de dangers, les pages d'hameçonnage en français constituent la plus grande part de la collecte (92 %). L'hameçonnage, qui avait longtemps épargné les internautes francophones, représente maintenant la majorité des attaques.

Les utilisateurs de PayPal, cible n° 1 des cybercriminels

Dans le secteur de l'hameçonnage, les fausses pages prenant pour cible les utilisateurs francophones de PayPal représentent une écrasante majorité (67 %). Ces pages en langue française sont liées à des courriels d'hameçonnage. Ils invitent les utilisateurs à se connecter à leur compte pour effectuer diverses actions (vérification des débits suite à une « charge inhabituelle » sur la carte bancaire, réinitialisation des mots de passe...).

Les coordonnées des comptes PayPal saisies sur ces fausses pages web sont automatiquement volées à leur propriétaire afin d'y récupérer l'argent stocké. Cette forte proportion de sites d'hameçonnage liés à PayPal s'explique par l'intérêt de ce type de système pour l'économie cybercriminelle. Un compte PayPal volé peut avoir de multiples usages, tels que le transfert d'argent ou l'escroquerie sur des sites de ventes aux enchères. Dans un registre équivalent, les faux sites eBay représentent 3 % des pages françaises dangereuses. eBay et PayPal, une combinaison idéale pour tout cybercriminel souhaitant escroquer des internautes.

Attention! Votre Compte PayPal à été limité!

De : **Compte PayPal** (service@paypal.fr)
Ce message provient peut-être d'un usurpateur. [En savoir plus](#)
Envoyé : jeu. 08/04/10 03:22
À : [adresse masquée]

PayPal



Cher utilisateur PayPal:

Attention! Votre Compte PayPal à été limité!

Dans le cadre de notre sécurité Mesures, nous procédons régulièrement à l'activité de l'examen PayPal d'apprendre reconnaître. Vous ont contacté après avoir relevé un problème sur votre compte, sur la demande des informations auprès de vous pour la raison suivante:

-Notre système a détecté charges inhabituelles à une carte de crédit liée à votre Compte PayPal.

[Cliquez ici pour activer votre compte](#)

Cordialement,

PayPal Email ID: 5138-8872

Département de l'examen des comptes de PayPal.

Le Corp Copyright 2002-2012 PayPal PayPal. Tous droits réservés.

Les courriels d'hameçonnage en français liés à PayPal sont très courants. Les liens insérés dans ces courriels pointent vers les faux sites Internet.

Les organismes français n'échappent pas à l'hameçonnage

Les organismes français faisant l'objet d'usurpation (banques et organismes d'états) représentent 11 % des dangers susceptibles d'être rencontrés par des internautes francophones. Durant la période de l'étude, le site de la Caisse d'Allocations Familiales et celui de la Caisse d'Épargne ont connu une attaque d'hameçonnage significative. Notons que les pages d'hameçonnage d'organismes français sont peu présentes sur des adresses .fr. Pour allonger le délai de blocage de ces pages frauduleuses et complexifier d'éventuelles enquêtes policières, le stockage de ces pages sur

des sites étrangers est privilégié par les cybercriminels. C'est ainsi que 9 % des adresses recensées et comportant l'extension .fr renferment des pages d'hameçonnage étrangères.

Les sites français, relativement épargnés par les malwares

Avec un taux de 8 %, les pages Internet françaises infectées par des malwares représentent une faible part des dangers. Un point encourageant pour les internautes francophones, mais qui doit tout de même être relativisé, car les techniques d'infection utilisées rendent difficile une collecte exhaustive. Peu de cybercriminels optent en effet pour une insertion pure et simple de code malveillant dans les pages Internet. En pratique, une fois le serveur Web contrôlé, le chargement du code nuisible à partir d'un autre serveur (via IFRAME ou SCRIPT, par exemple) est souvent envisagé. Une autre possibilité consiste à modifier les publicités des pages Web. Ces pages généralement mises à jour via IFRAME sont détournées. Ces deux techniques d'infection sont plus difficilement détectables, car elles permettent d'infecter un site Internet de manière aléatoire. Comme une bannière classique, son contenu peut provenir de plusieurs serveurs. Il en résulte ainsi une alternance entre page saine et page infectée. Dans le panel étudié, 87 % des pages web infectées l'étaient par iFrame...

Un bon surf n'est pas une garantie

Un autre point est à prendre en compte pour relativiser le faible taux d'infection des pages web française. Si au niveau mondial, les sites dangereux sont souvent identifiables (sites pornographiques ou de piratage) lorsque l'on se cantonne aux pages francophones collectées, la typologie change. Les pages en langue française hébergeant les dangers au sens large sont souvent des sites web grand public. Autrement dit, il ne suffit pas d'avoir une démarche de « bon père de famille » sur Internet pour éviter les dangers. Les sites de club sportif ou d'associations remontent par exemple très souvent dans les sites infectés. Les gros acteurs d'Internet et les portails des grandes entreprises semblent toutefois épargnés par les infections.

Quatre conseils pour un Internet plus sûr

1. Les mises à jour de sécurité des applications web, des logiciels de gestion et de création de pages Web doivent être réalisées quotidiennement. Ceci afin de combler les failles critiques avant qu'ils puissent être utilisés à grande échelle.
2. Les hébergeurs de site Web doivent régulièrement contrôler les versions hors ligne de leurs sites avec un module de balayage antivirus.
3. Les administrateurs de sites Internet doivent utiliser des mots de passe complexe pour sécuriser leurs accès FTP ou leur console de gestion de site Web. Rappelons qu'un mot de passe complexe doit comporter entre au moins 8 caractères et mélanger lettres (minuscules et majuscules), chiffres et symboles. Une démarche qui rend plus difficile les attaques automatiques dites par Dictionnaire.
4. Les créateurs et les administrateurs de sites Internet doivent s'assurer de la non-infection de leur système avant toute intervention sur leurs pages Web. Pour cela, l'installation d'un antivirus est nécessaire.

Cinq conseils aux internautes

1. Installez ou activez un filtre anti-hameçonnage dans votre logiciel de messagerie ou votre navigateur Internet.
2. Gardez votre système à jour, ainsi que toutes vos applications.
3. Ne cliquez pas sur un lien intégré dans un email provenant d'un organisme financier, d'Etat, de site marchand etc. En cas de doute sur la validité de ce courriel, la vérification des informations doit se réaliser par saisie manuelle de l'adresse de l'organisme dans le navigateur Internet.
4. Même si vous naviguez sur des sites apparemment sans risque, ne faites pas l'impasse sur un logiciel Antivirus. Utilisez un antivirus intégrant un filtre HTTP et gardez le programme continuellement à jour.
5. Sur votre ordinateur utilisez par défaut un compte utilisateur standard pour naviguer sur Internet. Avec un compte administrateur le risque d'exécution de code malveillant augmente.

À propos de G Data Software AG : Avec plus de 20 ans d'expérience dans la sécurité informatique, G Data est aujourd'hui un des leaders, présent dans plus de 60 pays. G Data réunit dans ses produits le meilleur de la technologie : par exemple la technologie DoubleScan (deux moteurs d'analyse indépendants), et la protection immédiate OutbreakShield... Depuis 5 ans, aucun autre éditeur de logiciels de sécurité européen n'a obtenu autant de distinctions nationales et internationales que G Data.