G Data

Livre blanc 04/2011

Attaques sur Internet

Ralf Benzmüller
G Data SecurityLabs

Whitepaper_04-2011

Go safe. Go safer. **G Data.**

Table des matières

1. Introduction

Pour beaucoup de personnes, il est impossible d'imaginer la vie d'aujourd'hui sans Internet. Il fournit de l'information, du divertissement et des possibilités de communication. Vous pouvez faire des achats, jouer, contrôler des transactions bancaires ou encore utiliser les services publics. Mais les cybercriminels emploient aussi très bien Internet. Ils détournent des ordinateurs, volent des données, des identités et utilisent des services Internet populaires pour distribuer de la publicité et du logiciel malveillant. Il y a quelques années, la majorité des malwares étaient distribués sous forme de pièces jointes à des emails. Depuis, les malfaiteurs se sont déplacés vers les sites Internet. Le but de ces bandits est de gagner autant d'argent que possible. Une économie souterraine florissante a été développée à cet effet : tout ce dont un cybercriminel a besoin pour ses activités douteuses est commercialisé. Ce livre blanc décrit les endroits où les cybercriminels attendent leur victime.

2. Comment rencontrer des sites malveillants ?

Les Cybercriminels doivent gagner le contrôle d'un serveur web et/ou injecter le code malveillant sur ce site Web pour distribuer le malware. La manière la plus facile pour un attaquant est de créer son propre site Web. Mais une méthode encore plus efficace est l'utilisation de gros serveurs web piratés. Ceux-ci permettent à un attaquant d'atteindre un grand beaucoup de personne avec ses codes malveillants. Cependant, il y a également des moyens pour leurrer des visiteurs sur des sites web inconnus.

2.1 Email

L'email reste un important moyen de diffusion de programmes malveillants. Les pièces jointes contenant des codes malicieux sont devenues plus rares, mais n'ont pas pour autant disparu. Récemment ils s'étaient encore diffusés sous forme de dossiers PDF ou de fichiers HTML, car ces formats de fichier sont faussement identifiés comme sans risque. Les manières dont un ordinateur devient infecté ressemblent à ceux sur des sites Web malveillants. Mais l'email peut faire bien plus. Des millions d'emails sont envoyés quotidiennement avec des liens vers des sites web malveillants. Ils arrivent en tant que nouvelles sensationnelles, messages d'erreur, avis, factures ou même actes d'accusation légaux et leurrent les destinataires par les liens vers les sites web infectés qu'ils contiennent.

Les fraudeurs par hameçonnage se comportent d'une manière semblable. Mais au lieu de distribuer des malwares par l'intermédiaire d'un lien vers un site Web, ils visent les données personnelles de leurs victimes. Les e-mails et les pages Internet qui y sont liées ressemblent généralement très bien aux e-mails et sites web originaux. Il y a quelques années, les fraudeurs par hameçonnage plaçaient exclusivement leurs vues sur les clients de banque. Maintenant la catégorie des sociétés visées est sensiblement plus large.

Le focus est maintenant mis sur les données d'accès :

- Des réseaux sociaux tels que Facebook, MySpace et Twitter
- Des services de paiement et de livraison tels que PayPal et DHL
- Des banques en ligne

- Des fournisseurs d'email tels que Yahoo! , Google ou MSN
- Des magasins et enchères en ligne (par exemple eBay)
- Des jeux sur Internet tels que World of Warcraft ou Habbo Hotel

En principe, n'importe quel service peut être compromis si leurs restrictions d'accès sont limitées par un nom d'utilisateur et à un mot de passe. Les données d'accès volées peuvent alors être employées pour diverses actions : envoi de Spam ; paiement ou envoi de marchandises volées, vendues sur les marchés parallèles.

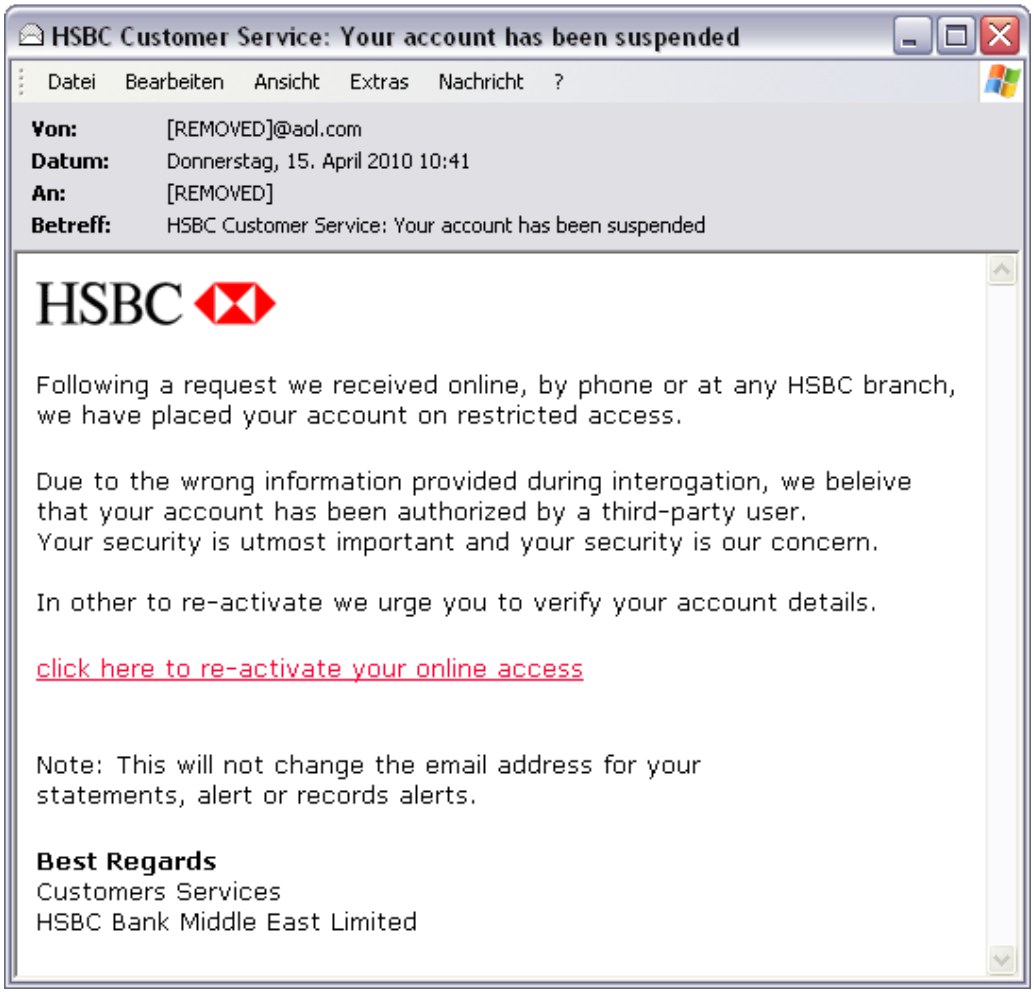


Illustration 1 : *Un email d'hameçonnage qui prétend provenir d'une banque officielle*

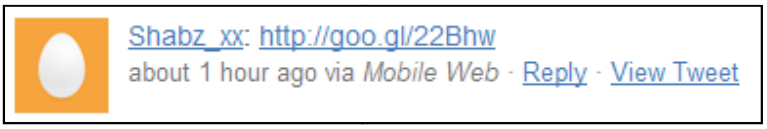
2.2 Risque sur le Web 2.0

L'Internet est un point de rencontre pour un grand nombre de personnes. Mais partout où les gens se rassemblent sur Internet, les risques sont présents. Ceci concerne la transmission de messages instantanés, les chatrooms, les réseaux sociaux, les forums, les blogs et les wikis.

Chatrooms et services de messagerie instantanée peuvent être exploités pour envoyer des liens vers des sites Internet malveillants. Des vers de messageries instantanées diffusent des liens vers des sites infectés après quelques commentaires d'introduction. Certains même verrouillent les communications entre un utilisateur et un chatroom et attachent le lien malveillant à une ou chacune des transmissions de l'utilisateur. Au-delà de l'infection, d'autres dangers existent. Les

informations de connexion sont stockées dans des cookies pendant toute la durée de la session. Dans certaines circonstances d'autres sites Web peuvent également accéder à ces cookies. Si ceci se produit, un attaquant peut envoyer des messages, changer des réglages ou lire les données - en fait toutes les actions permises par l'utilisateur – en utilisant le nom de la victime. Les cookies de session sont normalement supprimés quand l'utilisateur se déconnecte. L'usurpation n'est alors plus possible.

Des réseaux sociaux également sont exploités de plus en plus fréquemment pour la distribution de malware. Les messages des amis ont disposent généralement d'un haut niveau de confiance et sont donc cliqués plus fréquemment que dans les e-mails des individus inconnus.



Illusrtation 2: *En janvier 2011 un ver Twitter a employé le service de goo.g pour répandre un faux logiciel antivirus.*

Ceci rend les réseaux sociaux particulièrement attrayants pour les cybercriminels. Le ver Koobface est devenu spécialisé dans la distribution par l'intermédiaire des réseaux sociaux. Il envoie par exemple des messages avec des liens vers des vidéos supposées à tous les « amis » de la liste de contact sur Facebook, MySpace, Hi5, Friendster, Bebo, Twitter etc. La page vidéo demande alors à la victime de télécharger un lecteur Flash ou un codec vidéo. Tout internaute procédant à ce téléchargement intègre son ordinateur dans le botnet de Koobface.

N'importe quel utilisateur peut faire des entrées dans les forums, les blogs et les wikis – y compris les cybercriminels. Sur les réseaux parallèles, on commercialise des outils qui peuvent poster des entrées dans les forums ou les blogs de manière automatique. Les messages contiennent annonces publicitaires et/ou liens vers des sites web malveillants. Même le très populaire Wikipedia a été compromis. Dans un cas, il s'agissait d'un article concernant le ver Blaster contenant un lien censé mener vers un outil pour enlever ledit ver…

2.3 Faux résultats de recherche

Les cybercriminels ont une autre manière de conduire le trafic vers un site web malveillant. Des sites web peuvent être optimisés pour des recherches spécifiques de sorte qu'ils ressortent en top position sur certaines requêtes. Les cybercriminels tirent profit de ceci et optimisent des sites web malveillants pour certaines recherches spécifiques. Les termes choisis peuvent être dirigés vers des groupes ciblés – leurs favoris sont les jeux sur Internet et les contenus pornographiques.

Mais ils peuvent également utiliser des sujets d'actualité. Ceci est possible en évaluant des hitlists des termes les plus recherchés sur Google, Facebook, Twitter, etc. Ainsi, un site web malveillant peut par exemple être optimisé en utilisant le Google Trends. Naturellement, Google et les autres sociétés de moteur de recherche tentent de filtrer ces emplacements malveillants, mais ce n'est pas toujours réussi. En octobre 2010, Fabrice Jaubert de Google expliquait pendant la SecTor conférence que 1,5% de toutes les requêtes émises sur Google menaient à des sites Web malveillants.

2.4 Sites Internet piratés

Les informations ci-dessus sur la distribution des codes nuisibles supposent que les cybercriminels créent leurs propres serveurs web. Mais ce n'est pas toujours nécessaire. Un attaquant peut également rendre le malware disponible sur un serveur web connu, mais détourné. Il y a un certain nombre de méthodes pour réaliser ceci. Le Open Web Application Security Project (OWASP) est une organisation à but non lucratif qui produit des statistiques régulières sur les causes des attaques réussies sur des serveurs web. L'extrait du top 10 de l'OWASP dans le tableau 1 inclut une description des six types d'attaque les plus communs.

Rang	Risques de sécurité	Description
1	Injection	Les vulnérabilités d'injection concernent les systèmes de bases de données (SQL), les données d'ouverture (LDAP) et les fonctions. Elles se produisent quand des données d'utilisateur sont insuffisamment filtrées et le code généré par la requête peut être exécuté. Ceci permet à un attaquant d'accéder à des données sans autorisation ou même d'effectuer une attaque sur le serveur
2	Cross Site Scripting (XSS)	Le Cross Site Scripting est possible lorsque la saisie d'un utilisateur est de nouveau affichée sur une page ultérieure et que l'absence de contenu exécutable au niveau de la saisie n'est pas vérifiée. Prenons l'exemple du nom d'un formulaire qui est de nouveau affiché lors de la commande suivante. Si le pirate saisit un code JavaScript à la place de son nom, le code est, dans la mesure où il n'est pas filtré, exécuté par le navigateur.
3	Hacking d'authentification & de Session	Les insuffisances dans la gestion d'authentification et de session permettent à des attaquants de voler des mots de passe ou d'exploiter des données de chiffrage ou de session afin d'exécuter des actions sous les noms d'autres utilisateurs.
4	Insecure Direct Object Reference	Si les privilèges pour l'accès aux objets tels que les dossiers, les annuaires, les clés de base de données, etc. ne sont pas suffisamment signés dans le WebApp, un attaquant peut les manipuler.
5	Cross Site Request Forgery (SCRF)	Dans une attaque de CSRF, une requête HTTP est enregistrée par l'attaquant au nom de l'utilisateur qui a ouvert une session. Les WebApps vulnérables ne peuvent pas distinguer les fausses demandes des légitimes. L'attaquant dispose des mêmes droits que l'utilisateur autorisé. Il peut par exemple envoyer des messages, configurer le routeur, ou effectuer des achats ou des transactions financières.
6	Absence de configuration	La sécurité est souvent une question de configurations. Les serveurs Web, les bases de données, les WebApps et les plates-formes insuffisamment configurés offrent de nombreuses cibles pour l'attaque - particulièrement quand les configurations par défaut ont été maintenues.

Tableau 1: *Les six risques de sécurité les plus communs pour les serveurs web selon le Top 10 de l'OWASP*

Les applications Web populaires telles que les CMS, les boutiques en ligne, les wikis ou les systèmes d'affichage de contenu, qui sont employés sur la majorité des serveurs web, sont principalement concernées par ces attaques. Si une de ces applications contient une faille de sécurité, elle peut être exploitée. Les domaines qui utilisent de tels logiciels peuvent être identifiés en saisissant des requêtes spécifiques dans des moteurs de recherche. Les attaquants utilisent la liste de résultats et des outils appropriés pour lancer des attaques ciblées sur des serveurs. Si l'attaque est réussie,

n'importe quel malware peut être installé sur le serveur. De temps en temps c'est techniquement très complexe, mais même les nouveaux venus peuvent maîtriser cette complexité.

Les kits d'exploit Web offrent un paquet d'outils qui permettent d'effectuer les modifications nécessaires au déploiement de malware dans les serveurs attaqués. La mise en place de l'attaque et l'exploitation de nombreuses failles sont automatisées dans de tels outils. Ils exigent seulement la connaissance de quelques bases techniques. Les kits d'exploit Web tels que Fragus, Eleonore, Neosploit, etc. offrent un simple guide et des évaluations statistiques des ordinateurs infectés pour un prix à partir de 500 $. Les failles de sécurité intégrées sont souvent anciennes. Cependant, pour un léger surplus, la majorité des kits d'exploit fournissent des mises à jour régulières qui contiennent les nouvelles failles de sécurité. L'attaquant peut définir quelle attaque réalisée et quel fichier charger dans l'ordinateur si l'attaque a réussi. De tels outils permettent à des attaquants techniquement inexpérimentés de prendre part au marché parallèle de la cybercriminalité en transformant les ordinateurs infectés en « malware spray guns ».

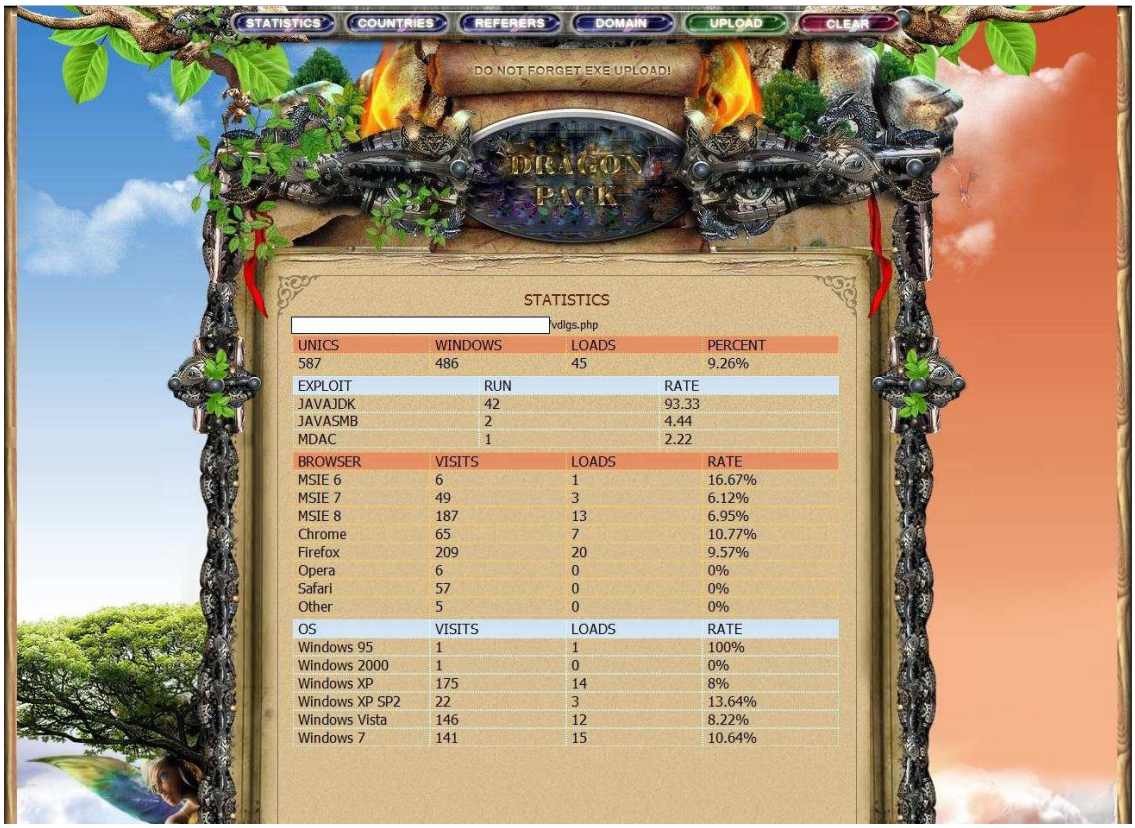


Illustration 1: *L'interface administrateur du web exploit "Dragon Pack" montre les statistiques*

2.5 Malvertising – Les bannières publicitaires infectées

Naturellement, les cybercriminels veulent gagner le contrôle d'un nombre important de serveurs web, comme ceux de journaux, de site d'actualités ou de portails Internet, afin d'atteindre le plus de victimes possible. Mais ce sont précisément les serveurs les mieux protégés. Il y a pourtant une manière d'y arriver. Car la plupart des sites Web sont financés par la publicité. Le contenu des annonces est généralement stocké sur des serveurs web spéciaux (appelés les adservers) et de là intégré dans les pages des sites Web. Les opérateurs de tels sites partent du principe que les

mesures du contrôle des prestataires de service de publicité sont suffisantes. Cependant, si les serveurs des sociétés de publicités sont piratés, les bannières Web peuvent être manipulées. Ceci s'est produit dès 2004 avec Falk eSolutions, dont les serveurs ont livré des bannières de publicité malveillantes à des sites anglais d'actualité tels que The Register.

Mais même lorsque les adservers sont bien protégés, les attaquants arrivent toutefois à glisser des bannières malveillantes simples à travers le flux des annonceurs. Et il n'est malheureusement pas facile de détecter ces malwares dans la pléthore de nouvelles bannières publicitaires journalières. Les composants Javascript ou Flash dans les bannières peuvent de plus fortement obscurcir leur code, ce qui rend difficile la détection de fonctions malveillantes. En outre, les codes peuvent être programmés de telle manière qu'ils deviennent seulement actifs dans certaines circonstances (par exemple date, nombre d'impressions, etc.). Ces techniques rendent tous les portails vulnérables. L'année dernière MySpace, New York Times, MSN Norvège, zeit.de et handelsblatt.de en ont fait les frais.

3 Attaque de l'Internaute

Jusqu'ici nous avons considéré la façon dont les internautes arrivent sur des sites Web malveillants. Mais que se produit-il ensuite ?

3.1 Anatomie d'une attaque

Le point de départ est l'une des sources mentionnées dans la section précédente. Dans le cas le plus simple, le lien pointe directement vers un fichier malveillant. Selon le navigateur et ses réglages, l'utilisateur est alors invité à télécharger et/ou exécuter le fichier. En fonction du choix, l'ordinateur est infecté plus ou moins rapidement. Une autre méthode consiste à utiliser un lien qui pointe directement vers un site Web infecté, une « landing page ». Ici l'utilisateur peut être invité à effectuer des actions spécifiques, telles que l'installation d'un programme infecté camouflé dans un faux antivirus. Mais des actions peuvent aussi être entreprises en arrière-plan et sans prévenir l'utilisateur, pour tenter d'utiliser des vulnérabilités sur l'ordinateur de l'internaute. Ces deux situations seront traitées plus en détail dans les paragraphes suivants, si ceci est fait directement, par l'interaction d'utilisateur ou de manière silencieuse.

Dans un cas typique, le premier composant de malware à transférer dans l'ordinateur est un téléchargeur (downloader). Celui-ci vérifie le système et envoie des données au sujet de la configuration de l'ordinateur, du système d'exploitation et de la protection installée sur un serveur distant. Il reçoit alors une commande de téléchargement de logiciel additionnel (d'où l'appellation de « téléchargeur "). Normalement le premier composant téléchargé est un backdoor. Ceci livre complètement l'ordinateur aux mains du cybercriminel. Des commandes spécifiques sont alors utilisées pour permettre le téléchargement de fichiers additionnels ou la réalisation d'actions spécifiques sur l'ordinateur (par exemple le redémarrage, l'envoi de Spam, etc.). Le backdoor permet au spyware d'être employé pour dépister des données valables sur l'ordinateur. Ceci permet par exemple la récupération des adresses e-mail, des mots de passe ou des clefs d'enregistrement de logiciel. Les Keyloggers sont employés pour enregistrer des mots de passe pendant qu'ils sont saisis.

Les données volées sont transférées à un ordinateur dédié (Drop Zone ou zone de largage). Une fois que les données ont été volées, l'ordinateur est vérifié afin de voir s'il peut être employé pour davantage d'activité criminelle. Si la connexion internet est lente, elle est simplement employée pour distribuer le Spam ou comme proxy. Si la connexion internet est rapide, elle peut être employée pour accueillir des sites Web ou des copies pirates. Ceci signifie qu'à l'insu de l'utilisateur, son ordinateur est complètement intégré dans la structure cybercriminelle.

3.2 Le drive-by infection

Beaucoup de sites Web malveillants, particulièrement ceux où des kits d'exploit sont installés, essaient d'utiliser des failles de sécurité dans le navigateur ou ses composants pour compromettre les ordinateurs des visiteurs. Le visiteur ne reçoit habituellement aucun fichier infecté. Cette technique est désignée sous le nom « infection par drive-by ». Les failles de sécurité les plus souvent exploitées sont basées sur l'affichage d'un PDF ou de fichier Flash, des erreurs dans les processus des applets Java, ou les failles dans des lecteurs multimédias tels que QuickTime, Realmedia, etc. Des erreurs dans les processus graphiques sont également exploitées. Mais vous pouvez vous protéger. N'importe qui gardant son ordinateur et ses applications installées à jour peut éviter la majorité des tentatives d'infections par drive-by.

3.3 Les escroqueries les plus populaires

Quand les cybercriminels ne peuvent pas ou ne veulent pas employer des méthodes techniques pour accéder aux ordinateurs, les visiteurs sont dirigés vers des sites Web où le malware est exécuté par l'action de l'utilisateur. Ceci s'appelle le social engineering. Voici une liste des escroqueries les plus courantes :

- Les messages dans les e-mails promettent des films ou tout autre contenu multimédia à la mode. Mais sur la page, un message d'erreur apparait demandant l'installation d'un lecteur ou d'un codec. Ce fichier est en fait un code nuisible.
- Beaucoup de sites Web concernent le domaine du jeu. Les jeux de rôle en ligne tels que World of Warcraft sont particulièrement populaires. Les forums associés offrent parfois les outils pour accélérer ou optimiser le jeu - qui s'avèrent alors être des malwares.
- Certains sites Web essayent d'employer des moyens agressifs pour convaincre les utilisateurs que leur ordinateur est infecté par des virus (« scareware » ou « rogueware »). Il est alors amené à croire que l'ordinateur est analysé. Le système se révèle bien entendu totalement infecté et une solution est immédiatement offerte à l'installation. Une fois installé sur l'ordinateur, en plus d'infecter le système, le logiciel invite l'utilisateur à payer pour bénéficier d'une protection optimale. Mais en plus de perdre quelques dizaines d'euros, les données de cartes bancaires de l'utilisateur sont volées, tout ceci pour un logiciel qui ne dispose d'aucune protection contre les virus.

4 Conclusion

Internet est un endroit dangereux. Les sites Web malveillants ne sont pas réservés aux coins sombres du Web. Même la lecture quotidienne d'actualités, le chat, ou la recherche d'un produit ou d'une expression courante peuvent mener à des sites Web malveillants. Dans le pire des cas, l'utilisateur ne note même pas que l'infection a eu lieu. Mais il est possible de se protéger. La base consiste à utiliser un logiciel antivirus et un navigateur à jour. Car le navigateur est le passage le plus courant pour les malwares.

À propos de G Data Software AG

G Data Software AG dont le siège social est situé à Bochum (Allemagne), est un éditeur de logiciel innovant spécialisé dans les solutions de sécurité. Fondée en 1985, la société G Data a été pionnière dans la protection virale en développant le premier programme antivirus.

En plus d'être l'une des plus anciennes sociétés de logiciels de sécurité au monde, G Data a obtenu depuis 5 ans plus de distinctions nationales et internationales qu'aucun autre éditeur de logiciels de sécurité européen.

La gamme de produits se compose de solutions de sécurité pour des particuliers et les entreprises. Les solutions G Data sont disponibles dans plus de 90 pays.

Plus d'informations sur www.gdata.fr