



**Bitdefender<sup>®</sup>**

# **Résumé du rapport sur l'état des e-menaces au 2<sup>nd</sup> semestre 2011**

# Mentions légales

Les informations et les données exposées dans ce document reflètent le point de vue de Bitdefender® sur les sujets abordés à la date de sa publication. Ce document et les informations qu'il contient ne peuvent en aucun cas être interprétés comme un engagement ou un accord de quelque nature que ce soit.

Bien que toutes les précautions aient été prises lors de l'élaboration de ce document, l'éditeur, les auteurs et les collaborateurs se dégagent de toute responsabilité en cas d'erreurs et/ou d'omissions. Ils ne sauraient être tenus pour responsables des dommages consécutifs à l'utilisation des informations qu'il contient. De plus, les informations contenues dans ce document sont susceptibles d'être modifiées sans avertissement préalable. Bitdefender, l'éditeur, les auteurs et les collaborateurs ne peuvent garantir que ce document sera repris ultérieurement, ni qu'il fera l'objet de compléments ou de mises à jour.

Ce document et les données qu'il contient sont publiés à titre strictement informatif. Bitdefender, l'éditeur, les auteurs et les collaborateurs ne fournissent aucune garantie expresse, implicite ou légale relatives aux informations mentionnées dans ce document.

Le contenu de ce document peut ne pas être adapté à toutes les situations. Si une assistance professionnelle est nécessaire, les services d'un professionnel compétent doivent être sollicités. Ni Bitdefender, ni les éditeurs du document, ni les auteurs ni les collaborateurs ne peuvent être tenus pour responsables des préjudices pouvant résulter de la consultation du document.

Le fait qu'une personne ou une organisation, un travail individuel ou collectif, y compris des textes imprimés, des documents électroniques, des sites Web, etc., soient mentionnés dans ce document en tant que référence et/ou source d'information actuelle ou future, ne signifie pas que Bitdefender, l'éditeur du document, les auteurs ou les collaborateurs avalisent les informations ou les recommandations que peuvent fournir la personne, l'organisation, les travaux individuels ou collectifs, y compris les textes imprimés, les documents électroniques, les sites Web, etc.

Les lecteurs doivent également savoir que Bitdefender, l'éditeur du document, les auteurs ou les collaborateurs ne peuvent garantir l'exactitude d'aucune des informations fournies dans ce document au-delà de sa date de publication, y compris, mais non exclusivement, les adresses Web et les liens Internet indiqués dans ce document qui peuvent avoir changé ou disparu entre le moment où ce travail a été réalisé et publié et celui où il est lu.

Le respect de l'ensemble des lois internationales applicables au copyright émanant de ce document relève de la pleine et entière responsabilité des lecteurs. Les droits relevant du copyright restant applicables, aucune partie de ce document ne peut être reproduite, stockée ou introduite dans un système de récupération des données, ou transmise à quelque fin ou par

quelque moyen que ce soit (électronique, mécanique, photocopies, enregistrement ou autres), ou dans quelque but que ce soit, sans l'autorisation expresse et écrite de Bitdefender.

Bitdefender peut posséder des brevets, des brevets déposés, des marques, des droits d'auteur, ou d'autres droits de propriété intellectuelle se rapportant au contenu de ce document. Sauf indication expresse figurant dans un contrat de licence écrit émanant de Bitdefender ce document ne concède aucune licence sur ces brevets, marques, droits d'auteur ou autres droits de propriété intellectuelle.

Tous les autres noms de produits ou d'entreprises mentionnés dans ce document le sont à titre purement informatif et sont la propriété, et éventuellement les marques, de leurs propriétaires respectifs.

*Copyright © 2012 Bitdefender. Tous droits réservés.*

# Zoom sur les malwares

- Bien que corrigée en 2008, la fonctionnalité de détournement de l'Autorun continue à être la technologie des systèmes Windows la plus exploitée. La famille Autorun est suivie du ver Downadup (Conficker) qui constitue la deuxième menace la plus destructrice du 2<sup>nd</sup> semestre 2011. Il est intéressant de noter que ces deux malwares continuent à faire des ravages alors que leur code n'a pas été mis à jour depuis des années et que les gangs de cybercriminels les ayant créés ont très probablement disparu.
- Les réseaux sociaux et les sites Web infectés sont deux des principaux vecteurs d'infection. Les utilisateurs de Facebook, dont le nombre atteint presque les 800 millions, sont constamment incités à cliquer sur des vidéos racoleuses (des méthodes d'ingénierie sociale extrêmement virales redirigeant les victimes à l'extérieur du réseau social). Parallèlement, l'augmentation du nombre de services utilisant de nom de domaine de deuxième niveau (tels que co.cc et .co.tv) hébergeant des kits d'exploits Web ont tellement augmentés que le géant des moteurs de recherche, Google, a été contraint de désindexer l'ensemble des sites en co.cc. La cybercriminalité s'étant alors tournée vers d'autres SLD gratuits, cette mesure s'est révélée inefficace et les noms de domaines de deuxième niveau en co.cc ont retrouvé leur place dans l'index de Google.
- Les messages de spam contenant des malwares, qui avaient gagné du terrain au premier semestre 2011, ont continué à progresser rapidement. Les principales vagues de spam incluant des malwares envoyaient leurs messages au nom de l'Automated Clearing House, un service financier proposé par l'association américaine de paiements électroniques NACHA. À l'ouverture de la pièce jointe, un téléchargeur générique récupérait une variante du bot Zeus sur Internet et l'installait sur la machine locale.
- Les téléphones portables fonctionnant sous Android ont vu l'apparition de nouvelles menaces au cours du second semestre 2011 : des malwares élaborés,

comme l'application Android System Message qui enregistre les conversations entrantes et sortantes ou le cheval de Troie jSMShider qui détourne les messages SMS entrants. Fin décembre, Google a également retiré 22 applications différentes de l'Android Market, après avoir confirmé qu'elles exploitaient une vulnérabilité du système d'exploitation pour faire envoyer des SMS vers des numéros surtaxés à l'insu des utilisateurs. Ces applications ont été téléchargées plus de 14 000 fois avant leur retrait de l'Android Market.

# Prévisions concernant les e-menaces

L'année 2011 a été particulièrement riche en activités malveillantes. Elle a débuté sous le signe des détournements de données et des fuites d'informations en entreprises avec l'émergence de bots extrêmement sophistiqués tels que ZeroAccess et TDL4, et s'est achevée avec Duqu, « le fils de Stuxnet ».

Le nombre de malwares continuera à augmenter de façon endémique en 2012 pour atteindre le nombre de 90 millions d'échantillons recensés, soit presque 17 millions de malwares de plus qu'à la fin de l'année 2011. Ils apparaîtront essentiellement sous la forme d'anciens malwares repackagés pour éviter la détection et de menaces exploitant des vulnérabilités de type « zero-day » présentes dans les systèmes d'exploitation et les logiciels additionnels.

Les réseaux sociaux seront la cible prioritaire des créateurs de malwares en 2012. Avec plus de 800 millions d'utilisateurs actifs, Facebook est devenu la plus grande communauté du Web. Bien que l'entreprise ait amélioré significativement la protection des interactions entre les utilisateurs et ait réduit le temps de réponse entre l'apparition d'une menace et sa suppression, plus de 400 millions d'utilisateurs sont exposés en permanence à de nouvelles menaces ayant une durée de vie très courte. Nous prévoyons pour 2012 une intensification des scams sur Facebook et Twitter, ainsi que l'apparition d'une famille importante de malwares se diffusant via des liens infectés postés directement sur les murs des utilisateurs.

Le système d'exploitation Android est également devenu un acteur majeur des attaques en 2011 à mesure que de plus en plus de constructeurs de tablettes et de smartphones intègrent leur version de l'OS dans leurs matériels. Depuis son introduction en 2008, la part de marché d'Android n'a cessé d'augmenter de façon exponentielle, passant à 25% aux États-Unis et même à 50% au Royaume-Uni (pays dans lesquels la pénétration des smartphones est la plus forte). Parallèlement, le nombre de menaces ciblant le système d'exploitation Android a considérablement augmenté, de même que le risque de fuite de données personnelles.

Bitdefender estime que le nombre de menaces spécifiquement conçues pour Android augmentera de façon phénoménale en 2012, à mesure que le système d'exploitation progressera sur le marché des appareils entrée et moyen de gamme.

Les nouvelles technologies joueront également un rôle essentiel dans les incidents liés à des malwares. Parmi ces technologies, on dénombre :

## L'introduction de HTML5

Ce nouveau langage est actuellement pris en charge par les principaux navigateurs et offre de nouveaux niveaux d'interaction entre l'utilisateur et les sites Web. Si l'amélioration de l'interaction est le principal objectif du lancement d'une version majeure du populaire langage de balisage, les nouvelles fonctionnalités permettront aux cyber-escrocs de concevoir des scams plus efficaces contre les utilisateurs d'Internet via les « Notifications Web », de suivre les victimes avec les données de géolocalisation (en particulier si elles utilisent HTML5 sur leur smartphone) ou même, de lancer des attaques contre d'autres sites directement à partir du navigateur de la victime.

## IPv6 et la fin d'Internet

On devrait, au dernier trimestre 2012, assister à l'épuisement des adresses IP du système IPv4. Cette sérieuse limitation qui pourrait empêcher tout nouvel abonné d'accéder à Internet, a été anticipée depuis quelques temps avec le début de la mise en place du protocole IPv6. Ce nouveau protocole est supporté par la plupart des systèmes d'exploitation tels que Windows Vista, Windows 7, Mac OS/X, tous les matériels Linux et BSD. Les appareils compatibles IPv6 supportent par défaut la configuration automatique sans état ('Stateless') qui leur permet de communiquer avec d'autres appareils et services du réseau IPv6 sur le même segment du réseau en signalant leur présence via le protocole Neighbor Discovery Protocol (NDP). Ce processus automatisé peut cependant exposer les appareils du réseau aux attaquants ou, dans des situations extrêmes, permettre à un attaquant de prendre le contrôle complet du matériel d'un réseau.

Le trafic IPv6 supporte également IPSec, un mécanisme qui permet au trafic de circuler de façon chiffrée entre la source et la destination. Bien que cette fonctionnalité protège contre le sniffing du trafic, elle sera probablement exploitée par les cybercriminels pour masquer le trafic de botnets depuis et vers le centre de commande.

## Windows 8 et les exploits de type « zero-day »

Le nouveau système d'exploitation de Microsoft, Windows 8, sortira prochainement. Les versions sorties en avant-première sur les services Web de partage de torrents et de peer-to-peer sont en général des versions « repackagées » du système d'exploitation avec de nombreux malwares qui corrompent le système avant que celui-ci ne soit complètement chargé, compliquant ainsi la détection et la désinfection. Les vulnérabilités de logiciels tiers constitueront également un important vecteur d'infection car les « packs d'exploits » en tirent constamment profit.

## Les attaques de phishing ciblées basées sur des données partagées sur les réseaux sociaux

Les 800 millions d'utilisateurs actifs sur Facebook publient de nombreuses informations personnelles et professionnelles en ligne sur le réseau social et souvent, ces informations sont accessibles à des personnes qui ne font pas partie de leurs amis en raison de paramètres de confidentialité insuffisants. Ces informations feront augmenter le risque d'attaques de phishing ciblées en 2012.