**Le jeudi 7 avril 2009**

# *Les chevaux de Troie dominent encore le Top 10 BitDefender des e-menaces du mois d'avril*

***Bien que Conficker soit encore bien présent dans la liste, d'autres e-menaces commencent à utiliser des méthodes similaires pour se propager***

***BitDefender®*** a publié aujourd'hui la liste des dix menaces les plus dangereuses pour les utilisateurs d'Internet au cours du mois d'avril. À l'instar du mois de mars, le sommet du classement est toujours dominé par les **chevaux de Troie**. Ces menaces, dont le mode de fonctionnement est de piéger les utilisateurs pour accélérer leur propagation, occupent sept des dix premières places du classement de ce mois-ci.

Seuls quelques vers, exploits et virus parviennent à rompre la « grande parade » des chevaux de Troie.

La présence en dixième position d'un cheval de Troie "silencieux", qui est injecté dans des sites Web officiels vulnérables, met en évidence l'importance du Web comme vecteur d'infection actuel. L'objectif recherché est que les navigateurs des visiteurs de ces sites Web chargent le code de l'exploit, comme c'est le cas avec les Trojan.Exploit.ANPW et Exploit.SWF.Gen, qui sont détectés par BitDefender et qui se placent respectivement en cinquième et sixième position dans le classement du mois d'avril. Cette combinaison existe réellement en ligne et se retrouve principalement sur des sites Web chinois malicieux.

**Trojan.Peed.Gen** (alias le redoutable « Storm Worm ») représente 1,81 % des détections du mois d'avril, mais c'est désormais un composant "dropper", c'est-à-dire qu'il dépose des virus au profit d'une menace différente. Cela indique que, bien qu'il soit toujours utilisé, l'efficacité de ce ver en tant que virus infectieux est révolue et qu'il est désormais utilisé uniquement pour la fonctionnalité de contrôle qu'il fournit aux cyber-attaquants.

Un nouveau venu se place en huitième position : Trojan.KillAV.PT. Cette menace est un logiciel malveillant "utilitaire" qui détruit tous les antivirus ou processus de sécurité (parmi une longue liste) qu'il peut trouver sur un ordinateur cible afin d'empêcher leur exécution. Ensuite, la menace décrypte et exécute un téléchargeur qui, à son tour, télécharge et installe un programme permettant de dérober les mots de passe utilisé dans des jeux.

À la septième place, Win32.Sality est le seul virus véritable du top 10 du mois d'avril. Win32.Sality est un virus polymorphe qui infecte les fichiers exécutables (.exe et .src) en les modifiant et en ajoutant son corps crypté dans une nouvelle section, à la fin de ces derniers. Ses autres moyens de diffusion consistent en une nouvelle (bien qu'ancienne) méthode : se combiner à un exécutable infecté dans le fichier Autorun.INF qui se trouve sur un média amovible ou des partages de réseau, une technique utilisée plus récemment par le ver Downadup / Conficker.

Le ver Conficker occupe la quatrième place, sous le nom de **Win32.Worm.Downadup.Gen**. Ses capacités sont à présent connues mais il est surprenant qu'après tout ce temps, il continue de se propager avec suffisamment de vigueur et représente à lui seul 3,05 % des détections.

*"Tout ce que nous pouvons espérer, c'est que ce taux de détection élevé soit dû aux personnes déjà infectées qui finissent par lancer une analyse avec un antivirus" a expliqué* Sorin Dudea, responsable

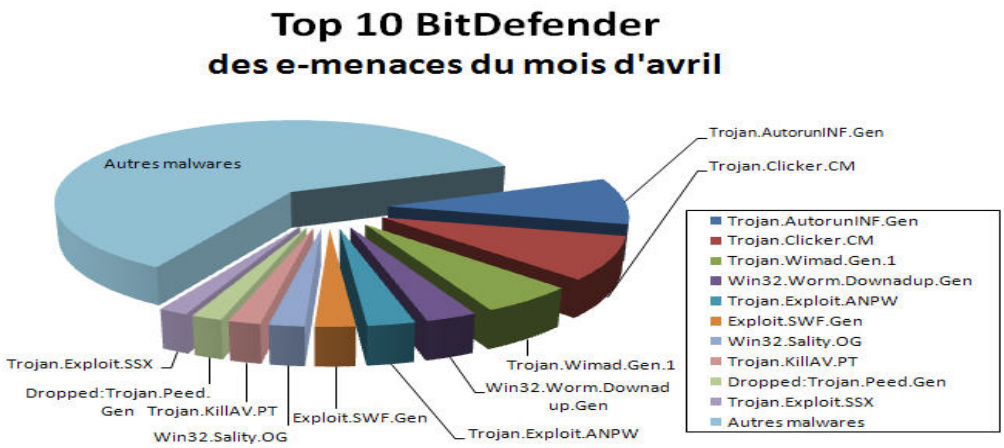
des Laboratoires de recherche antivirus BitDefender. *"Il est toutefois probable qu'en réalité le ver se réplique grâce à un réseau non négligeable d'ordinateurs infectés."*

Deux chevaux de Troie de type adware assez anciens, Wimad et Clicker, occupent la troisième et la deuxième place.

En première position se trouve Trojan.AutorunINF.Gen. Ce n'est pas une e-menace unique mais plutôt un nom générique de chevaux de Troie qui utilisent les mécanismes de propagation Autorun.INF décrits ci-dessus, mais pour lesquels une signature spécifique n'a pas été ajoutée.

*"Nous sommes plutôt satisfaits de l'utilisation de ce type de détection générique, sans intervention humaine. Et cela fonctionne bien."* confirme M. Dudea. *"Le futur de la détection antivirus fiable passe par l'adaptation aux nouvelles e-menaces en temps réel, et de telles techniques permettent d'ouvrir la voie."*

**Top 10 - BitDefender des principales e-menaces d'avril 2009 :**




### *À propos de BitDefender®*

*BitDefender est la société créatrice de l'une des gammes de solutions de sécurité la plus complète et la plus certifiée au niveau international reconnues comme étant parmi les plus rapides et les plus efficaces du marché. Depuis sa création en 2001, BitDefender n'a cessé d'élever le niveau et d'établir de nouveaux standards en matière de protection proactive des menaces. Chaque jour, BitDefender protège des dizaines de millions de particuliers et de professionnels à travers le monde – en leur garantissant une utilisation sereine et sécurisée de l'univers informatique. Les solutions de sécurité BitDefender sont distribuées dans plus de 100 pays via des partenaires revendeurs et distributeurs hautement qualifiés. Dans les pays francophones, BitDefender est édité en exclusivité par Éditions Profil. Plus d'informations sur BitDefender et ses solutions sont disponibles via le Centre de presse. Retrouvez également sur le site www.malwarecity.com les dernières actualités au sujet des menaces de sécurité qui permettent aux utilisateurs de rester informés des dernières évolutions de la lutte contre les malwares.*

### *À propos des Editions Profil*

*Editions Profil, société indépendante créée en 1989, développe, édite et diffuse des logiciels sur différents secteurs d'activités, professionnel et grand public. L'éditeur a constitué un large catalogue de solutions dans de nombreux domaines, par exemple sur les segments de la bureautique et de la productivité. Editions Profil s'est plus particulièrement spécialisée ces dernières années dans l'édition et la distribution d'outils de sécurité informatique et la protection des données en général. Editions Profil édite notamment les solutions de sécurité BitDefender et Parental Filter, ainsi que les solutions Farstone et diffuse les solutions de récupération de données et de gestion de serveurs MS Exchange de Kroll-Ontrack.*