Bitdefender : Les malwares en hausse de 23%, explications et dÃ©tails
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 7/2/2012 15:00:00

Une Ã©tude menÃ©e par Bitdefender annonce une augmentation de **23% des malwares en 2012** . Les malwares cibleront davantage les pÃ©riphÃ©riques Android et les rÃ©seaux sociaux. **Bitdefender**, Ã©diteur de solutions de sÃ©curitÃ©, prÃ©voit que le nombre de malwares augmentera de 17 millions environ par rapport Ã la fin de lâannÃ©e 2011 pour atteindre en 2012 le nombre de 90 millions, soit une hausse de **23%**.

Le rapport sur les e-menaces, Ã©laborÃ© au cours dâun an de dÃ©tection, de prÃ©vention et de dÃ©sinfection dans le monde entier comprend un aperÃ§u des dix principaux malwares en 2011, traite des Ã©volutions de âlâhacktivismeâ et de lâutilisation illÃ©gale de certificats numÃ©riques.

Ce rapport propose Ã©galement une analyse des messages de spam, qui ont reprÃ©sentÃ© **75,1%** de lâensemble des e-mails envoyÃ©s lâan dernier dans le monde.

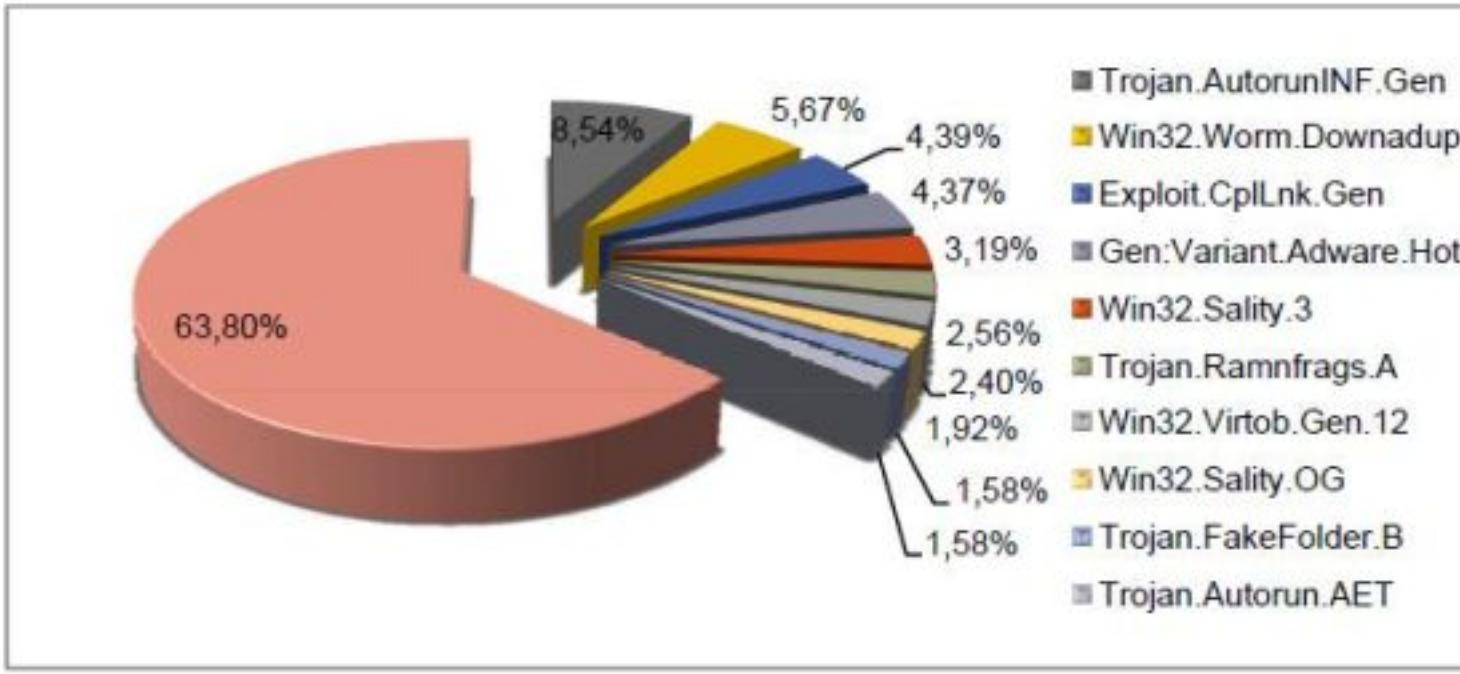
Zoom sur les malwares

â¢ Bien que corrigÃ©e en 2008, la fonctionnalitÃ© de dÃ©tournement de lâAutorun

continue Ã Ãªtre la technologie des systÃ¨mes Windows la plus exploitÃ©e. La famille Autorun est suivie du ver Downadup (Conficker) qui constitue la deuxiÃ¨me e-menace la plus destructrice du 2nd semestre 2011. Il est intÃ©ressant de noter que ces deux malwares continuent Ã faire des ravages alors que leur code nâ□□a pas Ã©tÃ© mis Ã jour depuis des annÃ©es et que les gangs de cybercriminels les ayant crÃ©Ã©s ont trÃ¨s probablement disparu.

â□¢ Les rÃ©seaux sociaux et les sites Web infectÃ©s sont deux des principaux vecteurs dâ□□infection. Les utilisateurs de Facebook, dont le nombre atteint presque les 800 millions, sont constamment incitÃ©s Ã cliquer sur des vidÃ©os racoleuses (des mÃ©thodes dâ□□ingÃ©nierie sociale extrÃªmement virales redirigeant les victimes Ã lâ□□extÃ©rieur du rÃ©seau social).

ParallÃ¨lement, lâ□□augmentation du nombre de services utilisant de nom de domaine de deuxiÃ¨me niveau (tels que co.cc et .co.tv) hÃ©bergeant des kits dâ□□exploits Web ont tellement augmentÃ©s que le gÃ©ant des moteurs de recherche, Google, Ã Ã©tÃ© contraint de dÃ©sindexer lâ□□ensemble des sites en co.cc. La cybercriminalitÃ© sâ□□Ã©tant alors tournÃ©e vers dâ□□autres SLD gratuits, cette mesure sâ□□est rÃ©vÃ©lÃ©e inefficace et les noms de domaines de deuxiÃ¨me niveau en co.cc ont retrouvÃ© leur place dans lâ□□index de Google.

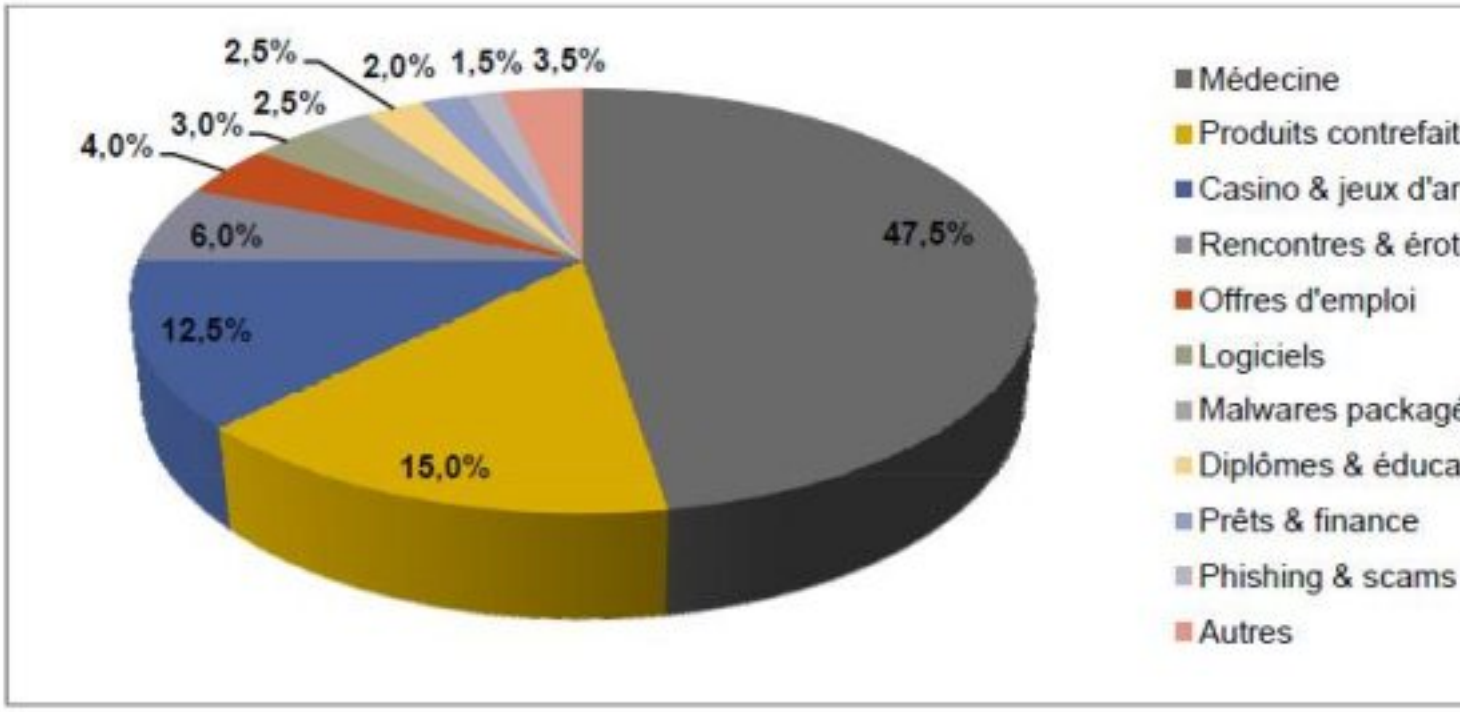


â□¢ Les messages de spam contenant des malwares, qui avaient gagnÃ© du terrain au premier semestre 2011, ont continuÃ© Ã progresser rapidement. Les principales vagues de spam incluant des malwares envoyaient leurs messages au nom de lâ□□Automated Clearing House, un service financier proposÃ© par lâ□□association amÃ©ricaine de paiements Ã©lectroniques NACHA. Ã lâ□□ouverture de la piÃ¨ce jointe, un tÃ©lÃ©chargeur gÃ©nÃ©rique rÃ©cupÃ©rait une variante du bot Zeus sur Internet et lâ□□installait sur la machine locale.

â□¢ Les tÃ©lÃ©phones portables fonctionnant sous Android ont vu lâ□□apparition de nouvelles menaces au cours du second semestre 2011 : des malwares Ã©laborÃ©s, comme lâ□□application Android System Message qui enregistre les conversations entrantes et sortantes ou

le cheval de Troie jSMSHider qui dÃ©tourne les messages SMS entrants. Fin dÃ©cembre, Google a Ã©galement retirÃ© 22 applications diffÃ©rentes de lâ□□Android Market, aprÃ¨s avoir confirmÃ© quâ□□elles exploitaient une vulnÃ©rabilitÃ© du systÃ¨me dâ□□exploitation pour faire envoyer des SMS vers des numÃ©ros surtaxÃ©s Ã lâ□□insu des utilisateurs. Ces applications ont Ã©tÃ© tÃ©lÃ©chargÃ©es plus de 14 000 fois avant leur retrait de lâ□□Android Market.

Lâ□□analyse du spam



Bien que lâ□□industrie du spam ait Ã©tÃ© affectÃ©e Ã de nombreuses reprises en 2011, notamment par la fermeture du plus grand service de spam affiliÃ© au monde (SpamIt) et par le dÃ©mantÃ¨lement de Rustock, le botnet le plus puissant et le plus efficace au monde, le spam a rÃ©ussi Ã maintenir un rythme relativement soutenu. Au second semestre 2011, lâ□□indice du spam atteignait **75,1%** du nombre total dâ□□e-mails envoyÃ©s dans le monde.

Ces donnÃ©es font partie du Rapport sur lâ□□Ã©tat des e-menaces, qui envisage lâ□□Ã©volution des malwares essentiellement sur les rÃ©seaux sociaux comme Facebook et Twitter, ainsi que sur les appareils mobiles, mais qui prÃ©dit aussi une hausse gÃ©nÃ©rale de la cybercriminalitÃ© :

Â« *Lâ□□annÃ©e 2012 connaÃ®tra une croissance explosive en termes de malwares, notamment en raison de la diffusion et du succÃ¨s croissant des rÃ©seaux sociaux* Â» dÃ©clare Bogdan Botezatu, analyste des e-menaces chez Bitdefender et chargÃ© de la coordination de ce rapport. Â« *Les malwares pour Android connaÃ®tront une croissance exponentielle, mais avec un volume initial bien plus faible* Â».

Pour retrouver Bitdefender en ligne