

Bitdefender : Les prÃ©visions des e-Menaces pour lâ€™annÃ©e 2012

SÃ©curitÃ©

PostÃ© par : JerryG

PubliÃ©e le : 22/12/2011 13:30:00

Lâ€™annÃ©e 2011 a Ã©tÃ© particuliÃ¨rement riche en activitÃ©s malveillantes. Elle a dÃ©butÃ© sous le signe des dÃ©tournements de donnÃ©es et des fuites dâ€™informations en entreprises avec lâ€™Ã©mergence de bots extrÃªmement sophistiquÃ©s tels que ZeroAccess et TDL4. Puis lâ€™annÃ©e sâ€™est achevÃ©e avec Duqu, Ã« le fils de StuxnetÃ».

Le nombre de malwares continuera Ã augmenter de faÃ§on endÃ©mique en 2012 pour atteindre le nombre de 90 millions dâ€™Ã©chantillons recensÃ©s, soit presque 17 millions de malwares de plus quâ€™Ã la fin de lâ€™annÃ©e 2011. Ils apparaÃ®tront essentiellement sous la forme dâ€™anciens malwares repackagÃ©s pour Ã©viter la dÃ©tection et de menaces exploitant des vulnÃ©rabilitÃ©s de type Ã« zero-day Ã» prÃ©sentes dans les systÃ¨mes dâ€™exploitation et les logiciels additionnels.



Les rÃ©seaux sociaux seront la cible prioritaire des crÃ©ateurs de malwares en 2012.

Avec plus de 800 millions dâ€™utilisateurs actifs, Facebook est devenu la plus grande communautÃ© du Web. Bien que lâ€™entreprise ait amÃ©liorÃ© significativement la protection des interactions entre les utilisateurs et ait rÃ©duit le temps de rÃ©ponse entre lâ€™apparition dâ€™une menace et sa suppression, plus de 400 millions dâ€™utilisateurs sont exposÃ©s en permanence Ã de nouvelles menaces ayant une durÃ©e de vie trÃ¨s courte. Nous prÃ©voyons pour 2012 une intensification des scams sur Facebook et Twitter, ainsi que lâ€™apparition dâ€™une famille importante de malwares se diffusant via des liens infectÃ©s postÃ©s directement sur les murs des utilisateurs.

Le systÃ¨me dâ€™exploitation Android est Ã©galement devenu un acteur majeur en 2011 et depuis son introduction en 2008, la part de marchÃ© dâ€™Android nâ€™a cessÃ© dâ€™augmenter de faÃ§on exponentielle, passant Ã 25% aux Ãtats-Unis et mÃªme Ã 50% au Royaume-Uni (pays dans lesquels la pÃ©nÃ©tration des smartphones est la plus forte). ParallÃ¨lement, le nombre de menaces ciblant le systÃ¨me dâ€™exploitation Android a considÃ©rablement augmentÃ©, de mÃªme que le risque de fuite de donnÃ©es personnelles.

Bitdefender estime que le nombre de menaces spÃ©cifiquement conÃ§ues pour Android augmentera de faÃ§on phÃ©nomÃ©nale en 2012, potentiellement jusqu'Ã 6 000%, en comparaison avec le nombre de menaces dÃ©tectÃ©es Ã fin 2011, Ã mesure que le systÃ©me d'exploitation progressera sur le marchÃ© des appareils entrÃ©e et moyen de gamme.

Les nouvelles technologies joueront Ã©galement un rÃ´le essentiel dans les incidents liÃ©s Ã des malwares.

Parmi ces technologies, on dÃ©nombre :

â€¢ L'Ã©volution de HTML5 . Ce nouveau langage est actuellement pris en charge par les principaux navigateurs et offre de nouveaux niveaux d'interaction entre lâ€™utilisateur et les sites Web. Si lâ€™amÃ©lioration de lâ€™interaction est le principal objectif du lancement d'une version majeure du populaire langage de balisage, les nouvelles fonctionnalitÃ©s 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 donnÃ©es de gÃ©olocalisation (en particulier si elles utilisent HTML5 sur leur smartphone) ou mÃªme, de lancer des attaques contre d'autres sites directement Ã partir du navigateur de la victime.

â€¢ IPv6 et la fin d'Internet . On devrait, au dernier trimestre 2012, assister Ã lâ€™Ã©puisement des adresses IP du systÃ©me IPv4. Cette sÃ©rieuse limitation, qui empÃªchera tout nouvel abonnÃ© d'accÃ©der Ã Internet, a Ã©tÃ© anticipÃ©e depuis quelques temps avec le dÃ©but de la mise en place du protocole IPv6. Ce nouveau protocole est supportÃ© par la plupart des systÃ©mes d'exploitation tels que Windows Vista, Windows 7, Mac OS/X, tous les matÃ©riels Linux et BSD. Les appareils compatibles IPv6 supportent par dÃ©faut la configuration automatique sans Ã©tat (Stateless) qui leur permet de communiquer avec d'autres appareils et services du rÃ©seau IPv6 sur le mÃªme segment du rÃ©seau en signalant leur prÃ©sence via le protocole Neighbor Discovery Protocol (NDP). Ce processus automatisÃ© peut cependant exposer les appareils du rÃ©seau aux attaquants ou, dans des situations extrÃªmes, permettre Ã un attaquant de prendre le contrÃ´le complet du matÃ©riel d'un rÃ©seau.

Le trafic IPv6 supporte Ã©galement IPSec, un mÃ©canisme qui permet au trafic de circuler de faÃ§on chiffrÃ©e entre la source et la destination. Bien que cette fonctionnalitÃ© protÃ©ge contre le sniffing du trafic, elle sera probablement exploitÃ©e par les cybercriminels pour masquer le trafic de botnets depuis et vers le centre de commande.

â€¢ Windows 8 et les exploits de type « zero-day » . Le nouveau systÃ©me d'exploitation de Microsoft, Windows 8, sortira lâ€™annÃ©e prochaine. Les versions sorties en avant-premiÃ©re sur les services Web de partage de torrents et de peer-to-peer sont en gÃ©nÃ©ral des versions « repackagÃ©es » du systÃ©me d'exploitation avec de nombreux malwares qui corrompent le systÃ©me avant que celui-ci ne soit complÃ©tement chargÃ©, compliquant ainsi la dÃ©tection et la dÃ©sinfection. Les vulnÃ©rabilitÃ©s de logiciels tiers constitueront Ã©galement un important vecteur d'infection car les « packs d'exploits » en tirent constamment profit.

[Pour retrouver Bitdefender en ligne](#)