Bitdefender : les prÃ©visions des e-menaces en 2013
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 14/1/2013 14:00:00

Bitdefender publie son rapport des e-menaces du 2Ã¨me semestre 2012 et ses prÃ©visions pour 2013. BitdefenderÂ®, Ã©diteur de solutions de sÃ©curitÃ©, indique que les e-menaces Ã©voluent en permanence pour tirer profit des opportunitÃ©s de diffusion offertes par les nouvelles technologies, ainsi que pour rÃ©pondre aux demandes des cybercriminels qui recherchent un niveau de sophistication de plus en plus Ã©levÃ©.

Outre les tendances que nous avons observÃ©es ces quatre derniÃ¨res annÃ©es, de nouveaux dangers sont susceptibles dâ□□apparaÃ®tre dans le monde virtuel en 2013.

Des malwares qui adoptent le modÃ¨le commercial des logiciels officiels

Certains groupes modernes de cybercriminels sont structurÃ©s dâ□□une maniÃ¨re similaire aux Ã©diteurs de logiciels officiels. AprÃ¨s avoir introduit avec succÃ¨s la R&D, les tests, le marketing et mÃªme le support technique, les cybercriminels Ã©voluent dÃ©sormais Ã un tout autre niveau, un niveau international. Les malwares modernes sont traduits dans plusieurs langues afin de couvrir de plus grandes zones gÃ©ographiques et de faciliter la comprÃ©hension de leur message par les utilisateurs. Certains ransomwares utilisent dÃ©jÃ cette technique et nous prÃ©voyons quâ□□elle sera la norme de facto cette annÃ©e.

Des attaques contre lâ□□hyperviseur

La virtualisation devenant la prochaine grande innovation pour des millions dâ□□utilisateurs du monde entier, les entreprises et services passant Ã des environnements virtualisÃ©s et utilisant de plus en plus le cloud, les cybercriminels tenteront de trouver de nouvelles faÃ§ons de corrompre le serveur tout entier et les machines virtuelles au-dessus de lâ□□hyperviseur.

Un nouveau systÃ¨me dâ□□exploitation mobile, de nouveaux problÃ¨mes

Outre le fait que la croissance exponentielle des malwares Android se poursuivra en 2013, la nouvelle annÃ©e verra Ã©galement lâ□□arrivÃ©e de Firefox OS, un systÃ¨me dâ□□exploitation pour mobiles conÃ§u Ã partir de standards Web ouverts. On estime que la part de marchÃ© de Firefox OS sera dâ□□environ 2% Ã la fin de lâ□□annÃ©e, et que ses utilisateurs seront alors exposÃ©s Ã toutes les failles de conception potentielles de ce nouveau systÃ¨me dâ□□exploitation

Les anciennes menaces rÃ©gressent, de nouvelles menaces se crÃ©ent

La part de marchÃ© de Windows 7 a finalement dÃ©passÃ© celle de Windows XP qui occupait cette place de longue date, ce qui provoquera dâ□□importantes Ã©volutions pour les e-menaces. Les menaces basÃ©es sur lâ□□Autorun disparaÃ®tront probablement au cours du dernier trimestre 2013, ainsi que le ver Downadup/Conficker qui Ã©tait liÃ© Ã lâ□□exploitation de cette technologie. Elles laisseront la place Ã des adwares gÃ©nÃ©riques et plus intrusifs, ainsi quâ□□Ã des vecteurs dâ□□infections basÃ©s sur des rootkits tels que ZeroAccess.

Des infections de PC et des gÃ©nÃ©rateurs de monnaie Ã©lectronique

Les Bitcoins occupant une place de plus en plus importante dans le systÃ¨me Ã©conomique mondial, les cybercriminels concevront probablement de nouvelles faÃ§ons de gÃ©nÃ©rer des Bitcoins sur des ordinateurs corrompus.

UEFI et Windows 8

Le lancement de Windows 8 se traduira probablement par lâ□□adoption massive de la technologie UEFI, qui succÃ¨de au BIOS existant depuis des annÃ©es, mais qui nâ□□est pas parvenue Ã sâ□□imposer jusquâ□□Ã prÃ©sent. De plus en plus de PC et de portables Ã©tant Ã©quipÃ©s de cartes-mÃ¨res UEFI, les cybercriminels porteront probablement leur attention sur un environnement plus permissif que le BIOS devenu obsolÃ¨te.

Windows 8 va devenir Ã©galement une cible privilÃ©giÃ©e. En 2013, on prÃ©voit que Windows 8 dÃ©passera Windows Vista en termes de part de marchÃ© et les cybercriminels rechercheront probablement des vulnÃ©rabilitÃ©s spÃ©cifiques Ã cette plateforme, que ce soit au niveau du noyau ou du navigateur Web. Ces vulnÃ©rabilitÃ©s seront cependant peu utilisÃ©es tant que le nouveau systÃ¨me dâ□□exploitation de Microsoft nâ□□aura pas Ã©tÃ© rÃ©ellement adoptÃ©.

Pour plus dâ□□informations, **le rapport complet** est disponible

Pour plus dâ□□informations sur les produits de **la gamme Bitdefender 2013**.