G-Data : Un Livre Blanc sur les risques encourus par les Internautes
SÃ©curitÃ©
PostÃ© par : JPilo
PubliÃ©e le : 8/4/2011 13:30:00

La majoritÃ© des infections sont aujourdâ□□hui rÃ©pandues par simple navigationÂ sur des sites Internet. Lâ□□actualitÃ© rÃ©cente de lâ□□attaque Lizamoon en est unÂ exemple frappant, G-DataÂ Ã©dite Un Livre Blanc sur les risques encourus par les Internautes

Si pour cette attaque, la technique dâ□□injection de scripts dans les bases de donnÃ©es SQL de sites Internet semble avoir Ã©tÃ© utilisÃ©e, dâ□□autres mÃ©thodes existent pour infecter les serveurs web et rÃ©pandre des codes malveillants sur Internet.

Dans son Livre blanc Â« **Attaques sur Internet** Â», G Data fait un point sur les risques encourus par les Internautes et prÃ©sente les techniques utilisÃ©es par les cybercriminels.

Difficile dâ□□imaginer la vie dâ□□aujourdâ□□hui sans Internet . Il fournit tout un ensemble de services qui sont devenus au fil du temps indispensables. Mais les cybercriminels utilisent aussi trÃ¨s bien Internet. Ils dÃ©tournent des ordinateurs, volent des donnÃ©es, des identitÃ©s et utilisent des services Internet populaires pour distribuer de la publicitÃ© et du logiciel malveillant. Il y a quelques annÃ©es, la majoritÃ© des malwares Ã©taient distribuÃ©s sous forme de piÃ¨ces jointes Ã des emails. Aujourd'hui, la majoritÃ© des dangers s'est dÃ©placÃ©e vers les sites Internet.

Ralf Benzmueller, Directeur du G Data SecurityLabs : Â« *La rÃ©cente attaque massive par injection de scripts dans des bases SQL de plusieurs milliers de serveurs Web fera sans doute date par son ampleur. Elle dÃ©montre une fois de plus la vulnÃ©rabilitÃ© dâ□□Internet, et plus particuliÃ¨rement des serveurs Web. Mauvaises configurations ou non-mises Ã jour rÃ©guliÃ¨res des systÃ¨mes, les propriÃ©taires de serveurs Web pÃªchent bien souvent par nÃ©gligence et exposent ainsi les Internautes Ã des infections. Pour assainir Internet, il faut que les Internautes sâ□□Ã©quipent dâ□□une solution de sÃ©curitÃ©, mais il faut aussi que les hÃ©bergeurs soient plus attentifs aux problÃ¨mes de sÃ©curitÃ© de leurs serveurs.* Â»

Dans son livre blanc Â« Attaques sur Internet Â» , G Data Software constate quâ□□il nâ□□existe pas une typologie de sites Ã risque. Des rÃ©seaux sociaux, aux blogs en passant par les sites dâ□□informations, aucun serveur nâ□□est Ã lâ□□abri dâ□□une injection SQL, dâ□□une attaque XSS ou dâ□□un malvertising (banniÃ¨res publicitaires infectÃ©es).

Des outils clÃ©s en main pour infecter les serveurs Web

G Data fait aussi le constat quâ□□il nâ□□est nullement utile dâ□□Ãªtre un spÃ©cialiste pour

sâ□□adonner Ã des activitÃ©s cybercriminelles telles que lâ□□infection de serveur Web. Sur les marchÃ©s parallÃ¨les cybercriminels des kits dâ□□exploits Web sont disponibles pour 500 $. Ces outils automatiques et documentÃ©s permettent Ã une personne mal intentionnÃ©e dâ□□analyser des serveurs Web Ã la recherche de failles et dâ□□infecter ensuite le systÃ¨me.

Anatomie dâ□□une attaque

Une fois site Internet infectÃ©, le cybercriminel nâ□□a plus quâ□□Ã attendre ses victimes. Dans le cas de lâ□□attaque Lizamoon, lâ□□infection Ã©tait basÃ©e sur lâ□□installation dâ□□un faux antivirus (scareware) sur lâ□□ordinateur. Dans dâ□□autres techniques telles que lâ□□infection dite par Â« Drive-by Â», sont aussi utilisÃ©es : la simple ouverture de la page Internet suffit Ã lâ□□insertion du code nuisible dans le systÃ¨me dâ□□exploitation de lâ□□Internaute.

Les bonnes pratiques pour se protÃ©ger

Face Ã cette situation, lâ□□internaute doit redoubler de prudence et appliquer les bonnes pratiques. Lâ□□utilisation dâ□□une solution de sÃ©curitÃ© est indispensable, mais ne suffit pas. Mettre Ã jour rÃ©guliÃ¨rement son systÃ¨me dâ□□exploitation, son navigateur Internet et les applications sensibles (lecteurs flash, PDFâ□¦) est une autre dÃ©marche Ã entreprendre.