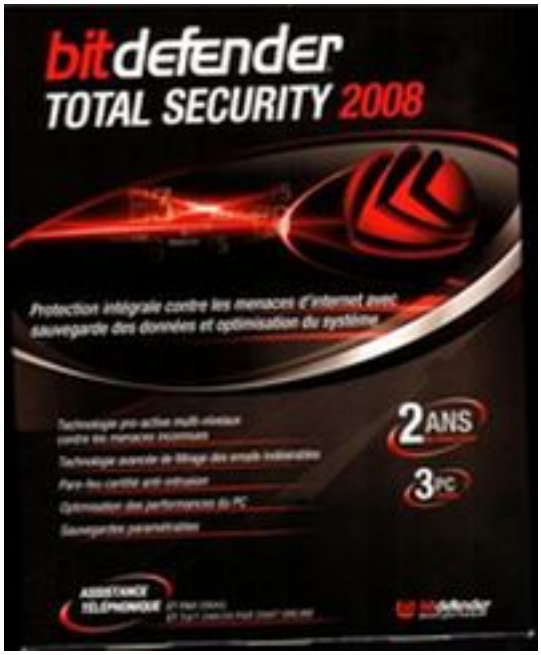
Le Top 10 des menaces de mai 2008 selon BitDefender
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 6/6/2008 0:00:00

BitDefenderÂ®, lâ□□un des fournisseurs les plus rÃ©compensÃ©s de solutions antivirus et de sÃ©curitÃ© des donnÃ©es, publie **le Top 10 des menaces les plus rÃ©pandues au mois de mai**.
Le haut du classement est largement dominÃ© par des **Trojans**, la plupart dâ□□entre eux ont Ã©tÃ© dÃ©couverts au cours des derniers mois - Ã l'exception notable de **Zlob**, un malware dÃ©tectÃ© depuis un certain temps dÃ©jÃ .



Â

Le Trojan.Downloader.WMA.Wimad.N arrive en seconde position et malgrÃ© un nom compliquÃ©, sa fonction est trÃ¨s simple : tÃ©lÃ©charger un autre malware. Ce quâ□□il effectue en feignant d'Ãªtre un assistant d'application tÃ©lÃ©chargeant un â□□**codec**â□□ pour lire un type particulier de fichier WMA.

Une fois l'utilisateur tombÃ© dans le piÃ¨ge, le Trojan tÃ©lÃ©charge puis lance **Adware.PlayMp3z.A**, une application destinÃ©e Ã voler les informations personnelles contenue dans lâ□□ordinateur Ã des fins commerciales ou potentiellement malhonnÃªtes.

Lorsquâ□□il est exÃ©cutÃ©, lâ□□adware va jusquâ□□Ã afficher un pop-up avec un accord de licence pour tenter de convaincre les victimes de sa lÃ©gitimitÃ©.

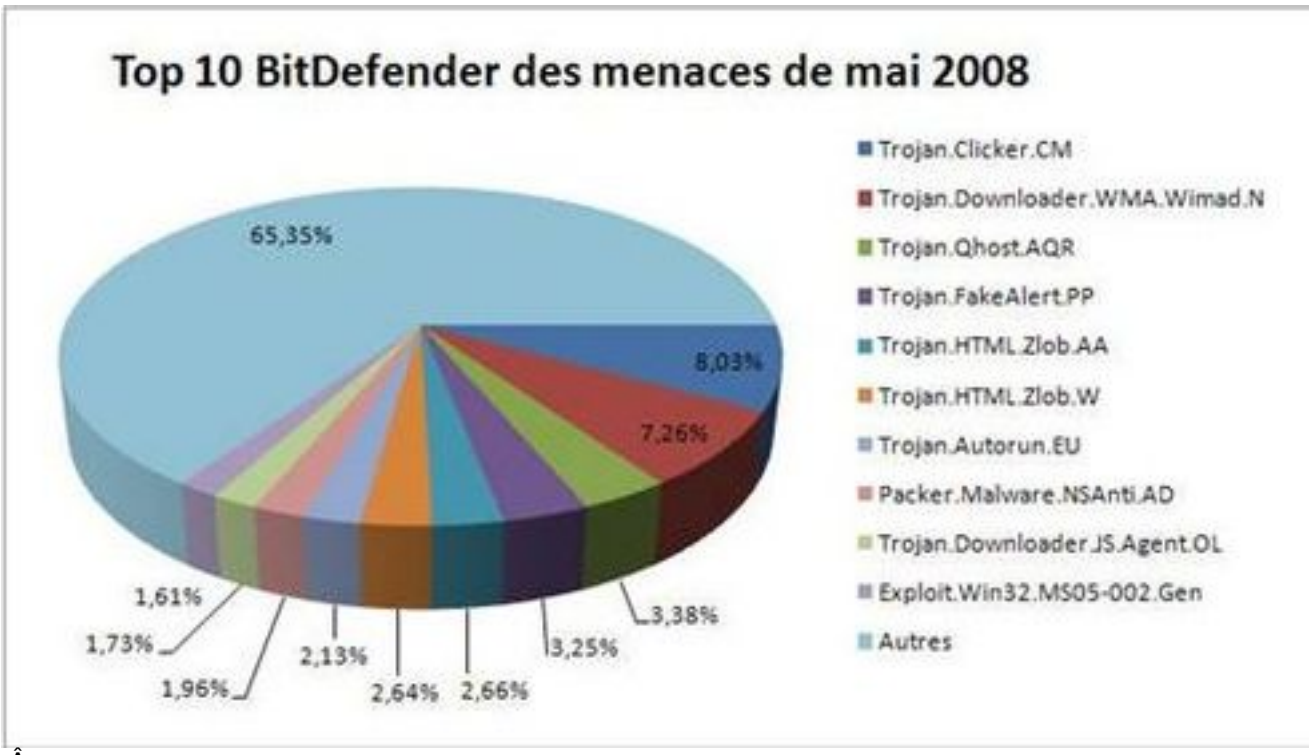
En premiÃ¨re position, le **Trojan.Clicker.CM** est un afficheur de pop-up intempestif, qui semble exploiter pleinement son code de contournement de Norton (il est programmÃ© pour pouvoir contourner le bloqueur de pop-up de Norton.)

Â

Contourner les protections des solutions de sÃ©curitÃ© semble Ãªtre en vogue puisquâ□□on retrouve en 3Ã¨me position un Trojan nâ□□ayant quâ□□un seul but : empÃªcher BitDefender de mettre Ã jour sa base de signatures virales. Il agit pour cela de maniÃ¨re ciblÃ©e, en modifiant le fichier Â« host Â» de la machine infectÃ©e.

Bien sÃ»r, cette technique ne fonctionne que sur les machines dont lâ□□analyse Ã lâ□□accÃ¨s nâ□□est pas activÃ©e.

Â« ***Cela prouve une nouvelle fois si nÃ©cessaire quâ□□il vaut mieux ne jamais dÃ©sactiver sa protection, mÃªme pour un court instant*** Â» commente **Sorin Dudea**, Directeur des Laboratoires Antivirus BitDefender.



Â

Le malware Packer NSAnti est toujours dans le top dix, grappillant mÃªme quelques points grÃ¢ce au nombre dâ□□auteurs de malwares qui tentent encore de cacher leurs crÃ©ations en utilisant cette technique.

En dixiÃ¨me position arrive de maniÃ¨re assez surprenante un â□□exploitâ□□ relativement ancien qui utilise un bug prÃ©sent dans le gestionaire des curseurs et des icÃ´nes de Microsoft Windows, cette faille pouvant permettre aux attaquants de prendre la main Ã distance sur les machines infectÃ©es.

Ce bug a Ã©tÃ© corrigÃ© depuis longtemps, mais il semblerait que de nombreux malwares incluent encore ce code malveillant juste Â« au cas oÃ¹ Â».

Le Top 10 BitDefender des malwares de mai 2008 :