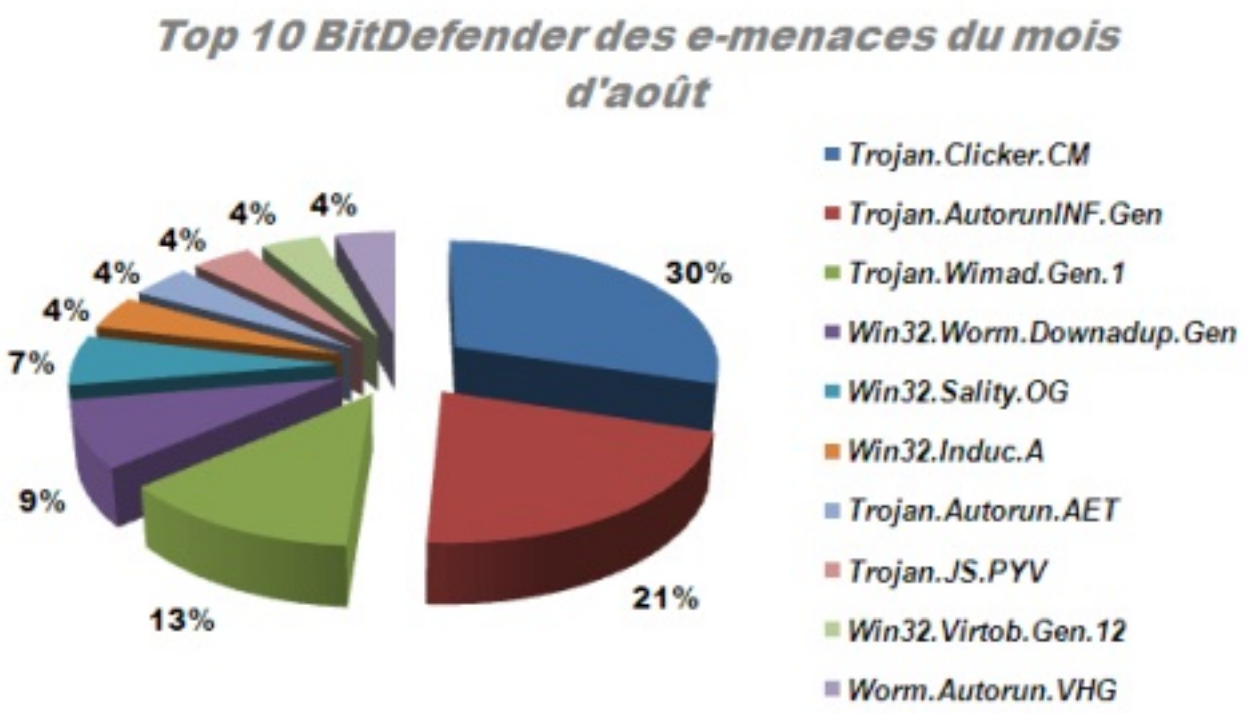
Le Trojan.Clicker.CM, 1 Ã¨re position au Top 10 BitDefender des menaces en aoÃ»t
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 3/9/2009 0:00:00

Trojan.Clicker.CM, en tÃªte de ce classement, est de plus en plus prÃ©sent sur les sites Internet de Â« warez Â» (portails de tÃ©lÃ©chargement hÃ©bergeant des cracks et des gÃ©nÃ©rateurs de clÃ©s pour les applications commerciales).
En deuxiÃ¨me position, **Trojan.AutorunINF.Gen** reprÃ©sente environ 10% de l'ensemble des infections. La fonctionnalitÃ© Autorun de Windows est utilisÃ©e par de nombreuses familles de malwares qui se propagent ainsi via des supports amovibles.

Trojan.Wimad.Gen.1 occupe la troisiÃ¨me position du classement du mois d'aoÃ»t avec 6% de l'ensemble des infections. Ce cheval de Troie affecte les fichiers ASF, qui ont la capacitÃ© de tÃ©lÃ©charger automatiquement des codecs vidÃ©o appropriÃ©s s'ils sont absents du systÃ¨me.

Les crÃ©ateurs de malwares modifient gÃ©nÃ©ralement ces fichiers afin qu'ils tÃ©lÃ©chargent Ã la place un fichier binaire malveillant.



Â

Â

En huitiÃ¨me position dans ce classement mensuel des e-menaces, **Trojan.JS.PYV** est un script malveillant affectant les utilisateurs consultant des sites Internet malveillants ou des sites Internet lÃ©gitimes compromis par des attaquants.

En neuviÃ¨me position se trouve Win32.Virtob.Gen, un infecteur de fichiers Ã©crit en langage

assembleur. Ce malware se camoufle en utilisant des process de Windows pour se lancer. Lâ□□attaque sâ□□effectue en temps rÃ©el en mÃ©moire et est dÃ©tectÃ©e immÃ©diatement par BitDefender Active Virus Control. Ce procÃ©dÃ© ne compromet pas les fichiers systÃ¨me, il les utilise.

Enfin, **Worm.Autorun.VHG**, est un ver de rÃ©seau/Internet qui exploite la vulnÃ©rabilitÃ© Windows MS08-067 afin de s'exÃ©cuter Ã distance en utilisant un package RPC (Remote Procedure Call, appel de procÃ©dure Ã distance) spÃ©cialement conÃ§u Ã cet effet (une technique Ã©galement utilisÃ©e par Win32.Worm.Downadup).

La prÃ©sence de ce ver dans le classement de BitDefender confirme que les utilisateurs ne prennent pas en compte les alertes de sÃ©curitÃ© de Microsoft et ne dÃ©ploient pas les patchs de sÃ©curitÃ©.

Marc Blanchard, EpidÃ©miologiste, Directeur des Laboratoires Editions Profil / BitDefender en France ajoute au sujet de lâ□□infection par Win32.Induc.OG qui corrompt les applications crÃ©Ã©es avec Delphi :

Â« *Cette mÃ©thode dâ□□infection apparue en 1997 et touchant les compilateurs Java de lâ□□Ã©poque refait son apparition avec les compilateurs Delphi. Le concept est dâ□□infecter les compilateurs eux-mÃªmes avant que les programmes soient compilÃ©s, ce qui permet de gÃ©nÃ©rer automatiquement une faille dans chaque programme compilÃ© avec ce compilateur compromis* Â».