BitDefender, Trojan.Clicker.CM conserve la premiÃ¨re place au Top 10
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 5/11/2009 0:00:00

Les chevaux de Troie continuent Ã dominer le Top 10 BitDefender des e-menaces en octobre Trojan.Clicker.CM, prÃ©sent principalement sur les sites Internet qui proposent des applications illÃ©gales telles que des cracks, des keygens et des numÃ©ros de sÃ©rie de logiciels commerciaux, occupe de nouveau, pour le mois dâ□□octobre cette fois-ci, la premiÃ¨re place du Top 10 BitDefender.

Il est gÃ©nÃ©ralement utilisÃ© pour afficher des publicitÃ©s dans le navigateur et reprÃ©sente 9,47% des fichiers infectÃ©s en octobre.

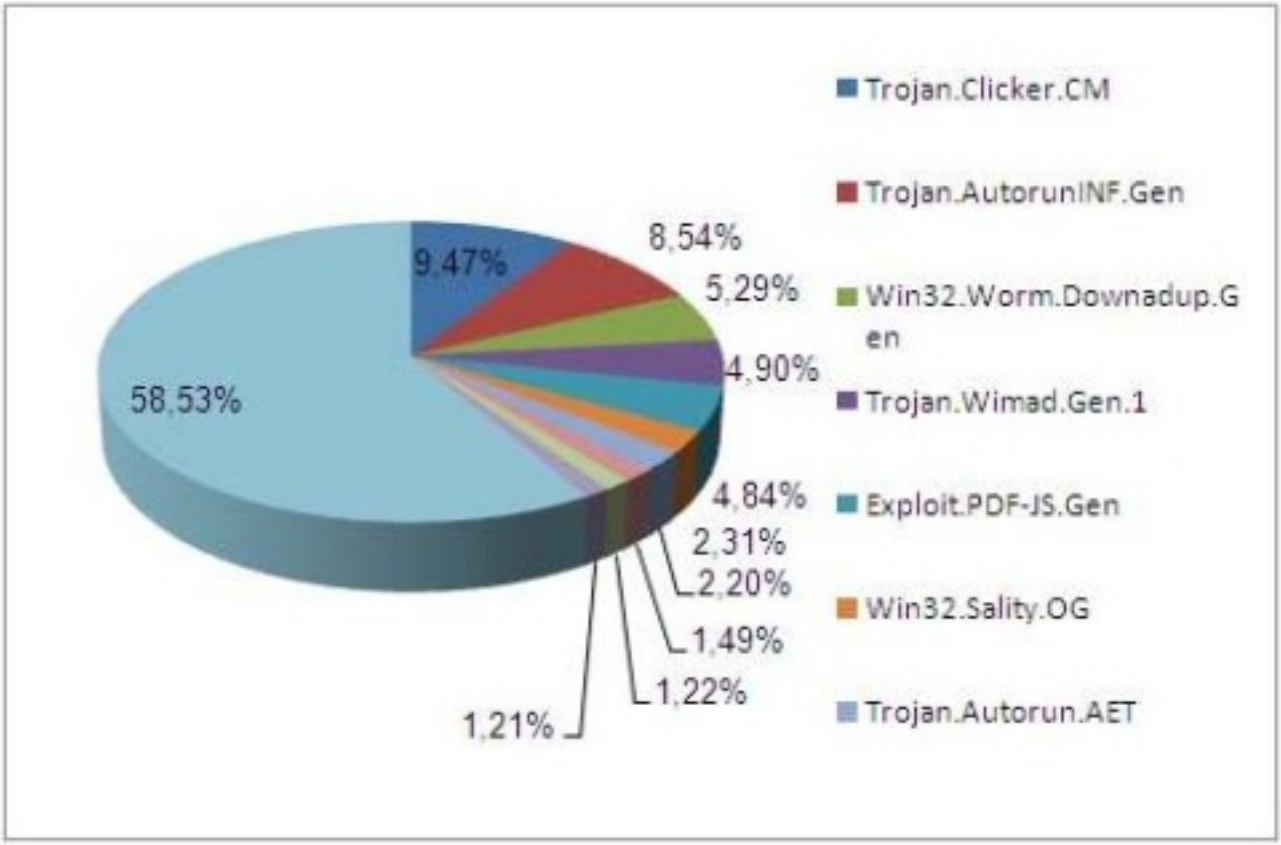
Trojan.AutorunInf.Gen, qui occupe la deuxiÃ¨me place avec 8,54% des infections, est un mÃ©canisme gÃ©nÃ©rique utilisÃ© pour diffuser des malwares via des supports amovibles tels que des clÃ©s USB, des cartes mÃ©moires ou des disques durs externes. Win32.Worm.Downadup et Win32.TDSS sont deux cÃ©lÃ¨bres familles de malwares qui utilisent cette approche pour causer de nouvelles infections.

Win32.Worm.Downadup se trouve en troisiÃ¨me position avec 5,29% de lâ□□ensemble des machines infectÃ©es. Aussi connu sous les noms de Conficker ou Kido, le ver bloque lâ□□accÃ¨s aux sites Internet de sÃ©curitÃ© informatique. Mais la derniÃ¨re version du ver va encore plus loin en installant de faux logiciels de sÃ©curitÃ© sur les machines compromises.

En quatriÃ¨me position, **Trojan.Wimad** reprÃ©sente 4,90% des infections. Il exploite une fonctionnalitÃ© moins connue mise en place par Microsoft afin de stocker des donnÃ©es multimÃ©dias synchronisÃ©es. Ce cheval de Troie affecte les fichiers ASF, un format dâ□□extension qui prend en charge la distribution de donnÃ©es sur une grande variÃ©tÃ© de rÃ©seaux tout en restant adaptÃ© Ã la lecture locale. Un fichier ASF spÃ©cialement corrompu exploite la fonctionnalitÃ© qui permet dâ□□installer des codecs appropriÃ©s pour installer Ã la place des

chevaux de Troie.

Sous le nom dâ**Exploit.PDF-JS.Gen**, en cinquiÃ¨me position, sont regroupÃ©s des fichiers PDF qui exploitent diffÃ©rentes vulnÃ©rabilitÃ©s dÃ©tectÃ©es dans le moteur Javascript de PDF Reader, afin dâexÃ©cuter du code malveillant sur lâordinateur de lâutilisateur. AprÃ¨s lâouverture dâun fichier PDF infectÃ©, un code Javascript spÃ©cialement conÃ§u Ã cet effet entraÃ®ne le tÃ©lÃ©chargement de binaires malveillants Ã partir dâemplacements distants. Cette menace correspond Ã 4,84% des infections mondiales.



Win32.Sality.OG, en sixiÃ¨me position avec 2,31% de lâensemble des infections, est un infecteur de fichiers polymorphe qui ajoute son code cryptÃ© aux fichiers exÃ©cutables (binaires .exe et .scr). Afin de ne pas se faire remarquer, il dÃ©ploie un rootkit sur la machine infectÃ©e et tente de supprimer les applications antivirus installÃ©es en local.

Trojan.Autorun.AET, en septiÃ¨me position avec 2,20% des infections totales, est un code malveillant qui se diffuse via les dossiers partagÃ©s de Windows et les supports de stockage amovibles. Ce cheval de Troie exploite la fonctionnalitÃ© Autorun des systÃ¨mes dâexploitation Windows pour lancer automatiquement des applications lorsquâun support de stockage infectÃ© est connectÃ©.

Worm.Autorun.VHG est un ver de rÃ©seau/Internet qui exploite la vulnÃ©rabilitÃ© Windows MS08-067 afin de sâexÃ©cuter Ã distance en utilisant un package RPC (remote procedure call) spÃ©cialement conÃ§u Ã cet effet (une technique Ã©galement utilisÃ©e par

Win32.Worm.Downadup). Le ver est huitiÃ¨me du classement avec 1,49% de lâ□□ensemble des infections.

Trojan.Swizzor.6 est une variante de la famille Swizzor, des tÃ©lÃ©chargeurs Â« cryptÃ©s Â» qui tentent dâ□□enregistrer et dâ□□exÃ©cuter de nouvelles menaces sur les machines infectÃ©es. Le cheval de Troie ajoute sa clÃ© au Registre Windows afin dâ□□exÃ©cuter une copie de lui-mÃªme Ã chaque fois que Windows est lancÃ©. Cette variante spÃ©cifique de Swizzor reprÃ©sente 1,22% des infections mondiales.

Enfin, la derniÃ¨re place du classement est occupÃ©e par Gen:Adware.Heur.wq0@j4oukhei, qui reprÃ©sente 1,21% de lâ□□ensemble des infections. Cette signature gÃ©nÃ©rique dÃ©tecte une large gamme dâ□□applications adwares, dont la famille NaviPromo.