

**BitDefender, Top 10 des mÃ©chants en septembre**

**SÃ©curitÃ©**

PostÃ© par : JerryG

PubliÃ©e le : 7/10/2009 0:00:00

En septembre encore, **les chevaux de Troie dominent le Top 10 de BitDefender**. Cinq e-menaces sur dix Ã©taient des chevaux de Troie en septembre

Les trois e-menaces en tÃªte du classement BitDefender de septembre sont des chevaux de Troie, qui reprÃ©sentent 25% du nombre total d'Ã©tats d'infections sur le mois. Le top 10 des e-menaces de BitDefender prÃ©sente les malwares les plus utilisÃ©s, dÃ©tectÃ©s par les chercheurs BitDefender.



En tÃªte du classement de septembre, Trojan.Clicker, un outil d'Ã©tats d'infection utilisÃ© par les dÃ©veloppeurs de malwares qui crÃ©ent des cracks, gÃ©nÃ©rateurs de clÃ©s, ainsi que des clÃ©s pour les principaux logiciels. Trojan.Clicker reprÃ©sente 10,98% des fichiers infectÃ©s.

La deuxiÃ¨me et la troisiÃ¨me place sont occupÃ©es par le cheval de Troie Wimad (9,58% des infections en septembre), nom gÃ©nÃ©rique regroupant les chevaux de Troie utilisant la fonction Autorun et par le cheval de Troie adware Clicker (5,52% des infections).

Conficker, dÃ©tectÃ© par BitDefender sous le nom de Win32.Worm.Downadup.Gen, prend la quatriÃ¨me place du classement avec presque 5,5% des fichiers infectÃ©s dÃ©tectÃ©s pour le mois de septembre.

L'Ã©tat d'exploit.PDF-JS.Gen, qui utilise une faille dans la faÃ§on dont certaines versions d'Adobe Reader analysent le code javascript insÃ©rÃ©, se retrouve en cinquiÃ¨me position avec 4,09% des infections.

L'Ã©tat d'exploit.JS.Y, un code Javascript malveillant gÃ©nÃ©ralement dÃ©tectÃ© dans des sites Internet compromis ou malveillants arrive en sixiÃ¨me position de la liste avec 3,44% des infections.

Le vÃ©tÃ©ran du top 10 de BitDefender, Win32.Sality.OG, est passÃ© de la cinquiÃ¨me Ã la septiÃ¨me place ce mois-ci avec 2,75% des infections.

*Top 10 BitDefender des e-menaces du mois de septembre :*

1. Trojan.Clicker.CM	10,98%
2. Trojan.AutorunINF.Gen	9,58%
3. Trojan.Wimad.Gen.1	5,52%

Trojan.Autorun.AET et Worm.Autorun.VHG, deux menaces qui utilisent la fonction Autorun (exÃ©cution automatique) dans d'anciennes versions de Windows, occupent la huitiÃ©me et la neuviÃ©me place de ce top 10 BitDefender de septembre. Il est intÃ©ressant de noter que Worm.Autorun.VHG est en fait un composant tÃ©lÃ©chargeur utilisÃ© pour diffuser le cÃ©lÃ©bre ver Conficker, aussi appelÃ© Kido ou Downadup.

Le classement s'achÃ©ve avec Trojan.Skintrim.HTML.A (1,29 % des infections totales), un type de page HTML associÃ© Ã des programmes adwares comme Navipromo.

Marc Blanchard, EpidÃ©miologiste et Directeur des Laboratoires Editions Profil / BitDefender en France dÃ©clare : Â« La recrudescence des infections actives via le web (HTTP) se confirme de mois en mois. L'exploitation des navigateurs et des visualisations de pages PDF permettent aux malwares de pÃ©nÃ©trer dans les systÃ©mes (ordinateurs) des internautes sans attaquer de maniÃ©re frontale les ordinateurs via le rÃ©seau internet. Ces exploitations permettront un passage tout en douceur d'une machine saine Ã une machine zombie. Une fois la machine exploitÃ©e, le malware se sert des unitÃ©s de masse USB (clefs, disques durs externes, etc) pour se propager via les Autoruns, car les Ã©changes de donnÃ©es par les clefs USB sont trÃ©s frÃ©quentes vu leurs importantes capacitÃ©s. C'est pourquoi trois trojan Autorun restent trÃ©s bien placÃ©s dans le top 10. Â»

Pour Ãªtre informÃ© des derniÃ©res e-menaces, [inscrivez-vous aux flux RSS BitDefender](#)