BitDefender : Les chevaux de Troie dominent encore le Top 5 de mars
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 7/4/2010 0:00:00

Les chevaux de Troie occupent la premiÃ¨re et cinquiÃ¨me place et deviennent ainsi le vecteur dâ□□infection principal de ce classement

BitDefenderÂ®, Ã©diteur de solutions de sÃ©curitÃ© anti-malwares publie aujourdâ□□hui le Top 5 des e-menaces du mois de mars.

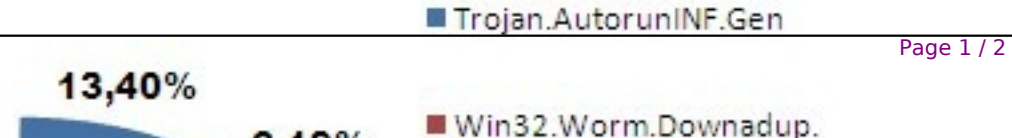
HabituÃ© de la premiÃ¨re place, Trojan.AutorunInf.Gen, mÃ©canisme gÃ©nÃ©rique se diffusant via des supports amovibles, se classe une nouvelle fois en tÃªte de ce classement mensuel avec 13,40% de lâ□□ensemble des malwares.

Avec **6,19%** des infections totales, Win32.Worm.Downadup.Gen, (aussi appelÃ© Kido ou Conficker), se maintient en deuxiÃ¨me position, comme au cours des trois derniers mois. Â« Ce ver exploite une vulnÃ©rabilitÃ© connue de MicrosoftÂ® WindowsÂ®. Pour Ã©viter dâ□□Ãªtre infectÃ©, il suffit de mettre Ã jour son systÃ¨me dâ□□exploitation et la solution de sÃ©curitÃ© installÃ©e sur son PC Â» explique Catalin Cosoi, chercheur des Laboratoires BitDefender.

La troisiÃ¨me e-menace de ce classement du mois de mars est Exploit.PDF-JS.Gen, qui manipule le moteur Javascript dâ□□Adobe PDF ReaderÂ® afin dâ□□exÃ©cuter du code malveillant sur les ordinateurs, avec 5,30% du total des infections.

En quatriÃ¨me position se trouve le seul infecteur de fichiers de ce classement : Win32.Sality.OG. Le code polymorphe des malwares appartenant Ã la famille Sality les rend extrÃªmement difficiles Ã dÃ©tecter et Ã supprimer. De plus, le virus tente de dÃ©sactiver une liste dâ□□antivirus potentiellement installÃ©s sur le systÃ¨me infectÃ©.

Le classement sâ□□achÃ¨ve avec Trojan.JS.Downloader.BIO, un code Javascript insÃ©rÃ© dans des pages web lÃ©gitimes via des techniques dâ□□injection SQL, ciblant uniquement les sites web conÃ§us en ASP. Il crÃ©e Ã©galement des cookies avec diffÃ©rentes informations sur la victime (les sites consultÃ©s et les horaires de connexion) et les envoie Ã un site Internet basÃ© en Chine.



Top 5 BitDefender des e-menaces du mois de mars 2010 :

1 - Trojan.AutorunINF.Gen 13,40%

2 - Win32.Worm.Downadup.Gen 6,19%

3 - Exploit.PDF-JS.Gen 5,30%

4 - Win32.Sality.OG 2,58%

5 - Trojan.JS.Downloader.BIO 2,13%

AUTRES 70,40%

Â« *Les technologies dâ□□infection via la fonction AUTORUN constituent un flÃ©au majeur pour les infections des ordinateurs via les pÃ©riphÃ©riques USB tel que : les clefs USB, les disques durs amovibles, les tÃ©lÃ©phones portables ou les lecteurs MP3. Par ailleurs, les infections issues de la navigation sur des sites Internet trouvÃ©s sur les moteurs de recherches tels que Google ou Yahoo Search sont Ã©galement considÃ©rables.* Â» insiste **Marc Blanchard**, Ã©pidÃ©miologiste et Directeur des Laboratoires Editions Profil pour BitDefender en France. Â« *Ce cumul de technologies (USB / internet) reprÃ©sente la majoritÃ© des infections aujourd'hui. Lâ□□utilisateur doit donc plus que jamais rester vigilent lors de son utilisation, veiller Ã disposer de la derniÃ¨re version de sa solution de sÃ©curitÃ© et de bases antivirales Ã jour.* Â»

Pour plus dâ□□informations concernant les produits BitDefender. Et pour rester au fait de lâ□□actualitÃ© des e-menaces, nous vous invitons Ã vous abonner au flux RSS BitDefender