BitDefender : Top 10 des mÃ©chants en 2009
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 14/1/2010 0:00:00

Exploit.PDF-JS.Gen met un terme Ã la domination des chevaux de Troie dans le **top 10 BitDefender de dÃ©cembre 2009. Un exploit PDF** prend la tÃªte du classement

La tÃªte du classement du top 10 de BitDefender est occupÃ©e par lâ□□e-menace Exploit.PDF-JS.Gen, qui reprÃ©sente 12,04% de lâ□□ensemble des infections. Sous ce nom sont regroupÃ©s des fichiers PDF qui exploitent diffÃ©rentes vulnÃ©rabilitÃ©s dÃ©tectÃ©es dans le moteur Javascript de PDF Reader, afin dâ□□exÃ©cuter du code malveillant sur lâ□□ordinateur de lâ□□utilisateur. AprÃ¨s lâ□□ouverture dâ□□un fichier PDF infectÃ©, un code Javascript spÃ©cialement conÃ§u Ã cet effet entraÃ®ne le tÃ©lÃ©chargement Ã distance de codes binaires malveillants.

Avec **8,15%** des infections, la deuxiÃ¨me e-menace de ce Top 10 du mois de dÃ©cembre 2009 est **Trojan.AutorunInf.Gen**, un mÃ©canisme gÃ©nÃ©rique de diffusion de malwares via des pÃ©riphÃ©riques amovibles tels que les clÃ©s USB, les cartes mÃ©moire et les disques durs externes. Win32.Worm.Downadup et Win32.TDSS sont deux des familles de malwares les plus connues qui utilisent cette approche pour propager de nouvelles infections.

Trojan.Clicker.CM est en troisiÃ¨me position ce mois-ci avec **7,90%** des infections totales. On le trouve principalement sur des sites Internet proposant des applications illÃ©gales telles que des cracks, des keygens et des numÃ©ros de sÃ©rie des logiciels commerciaux les plus prisÃ©s. Ce cheval de Troie est utilisÃ© principalement pour afficher des publicitÃ©s dans le navigateur des utilisateurs afin dâ□□obtenir un maximum de revenus par les publicitÃ©s.

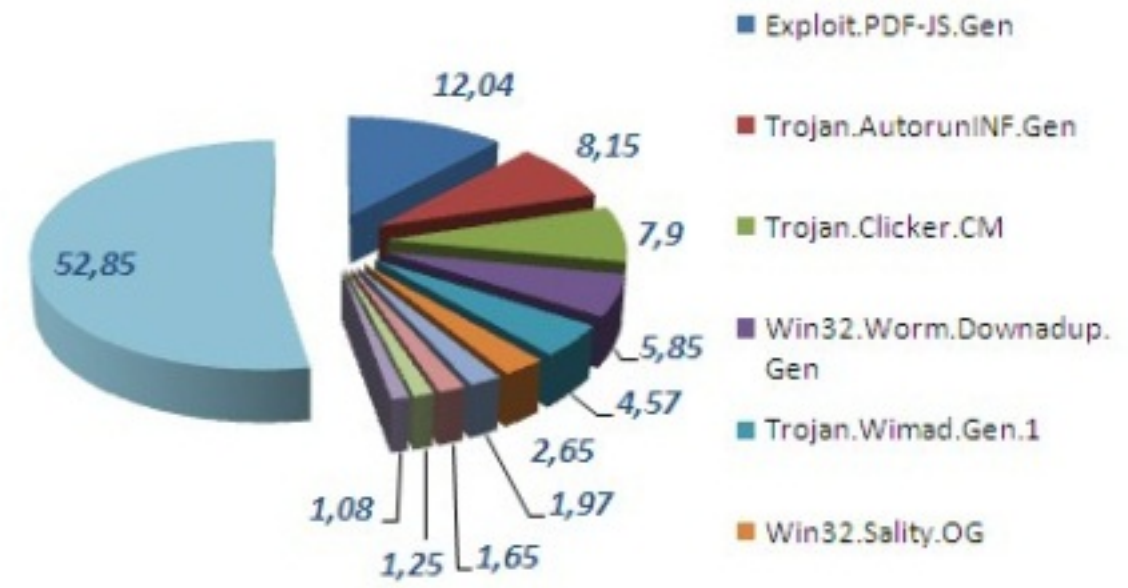
Ã□ lâ□□origine de **5,85%** des infections, **Win32.Worm.Downadup.Gen** occupe la quatriÃ¨me position du classement de ce mois. Ce ver exploite une vulnÃ©rabilitÃ© du service serveur RPC de Microsoft Windows permettant lâ□□exÃ©cution de code Ã distance (MS08-67) afin de se diffuser sur dâ□□autres ordinateurs du rÃ©seau local. Il restreint Ã©galement lâ□□accÃ¨s des utilisateurs Ã Windows Update et aux sites dâ□□Ã©diteurs de sÃ©curitÃ© informatique. De nouvelles variantes du ver installent Ã©galement de faux logiciels antivirus.

Trojan.Wimad.Gen.1 occupe la cinquiÃ¨me position avec **4,57%** de lâ□□ensemble des infections. Il exploite principalement la fonctionnalitÃ© permettant aux fichiers ASF de tÃ©lÃ©charger Ã

distance les codecs appropriÃ©s pour dÃ©ployer des fichiers binaires infectÃ©s sur lâ□□ordinateur hÃ´te. Le format ASF stocke des donnÃ©es aux formats WMA (Windows Media Audio) ou WMV (Windows Media Video), que lâ□□on trouve principalement sur les sites Internet de torrents. En lecture locale, ce fichier WMV spÃ©cialement conÃ§u tente de tÃ©lÃ©charger un Â« codec spÃ©cial Â» qui sâ□□avÃ¨re Ãªtre un code binaire malveillant provenant dâ□□un site tiers.

La sixiÃ¨me place, correspondant Ã **2,65%** des infections mondiales, est occupÃ©e par **Win32.Sality.OG**. Cette e-menace malveillante 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, elle dÃ©ploie un rootkit sur la machine infectÃ©e et supprime les applications antivirus en cours dâ□□exÃ©cution sur lâ□□ordinateur.

Trojan.Autorun.AET, en septiÃ¨me position avec **1,97%** 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 dâ□□exploitation Windows pour lancer automatiquement des applications lorsquâ□□un 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 sâ□□exÃ©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 **1,65%** de lâ□□ensemble des infections.

Win32.Worm.Downadup.B occupe la neuviÃ¨me position du classement avec **1,08%**. Câ□□est une

variante de Win32.Worm.Downadup avec pratiquement les mÃªmes fonctionnalitÃ©s, si ce nâ□□est que le nombre dâ□□URL de sites dâ□□antivirus bloquÃ©s est infÃ©rieur. Câ□□est Ã©galement lâ□□une des variantes les moins dangereuses, puisquâ□□elle nâ□□a pas de charge utile malveillante.

Le Top 10 du mois de dÃ©cembre 2009 sâ□□achÃ¨ve avec Trojan.Script.236197 .

Ã□ lâ□□origine de 1,08% des infections, ce fichier JavaScript Â« obscurci Â» affiche des fenÃªtres pop-up imitant les alertes MSN Messenger lorsque lâ□□utilisateur visite un site Internet pour adultes. Les publicitÃ©s, transmises via le service DoublePimp, ressemblent Ã une conversation en temps rÃ©el avec une femme censÃ©e se trouver dans la mÃªme zone gÃ©ographique que le fournisseur dâ□□accÃ¨s de lâ□□utilisateur.

Top 10 BitDefender des e-menaces du mois de dÃ©cembre 2009 :

1 Exploit.PDF-JS.Gen 12,04

2 Trojan.AutorunINF.Gen 8,15

3 Trojan.Clicker.CM 7,90

4 Win32.Worm.Downadup.Gen 5,85

5 Trojan.Wimad.Gen.1 4,57

6 Win32.Sality.OG 2,65

7 Trojan.Autorun.AET 1,97

8 Worm.Autorun.VHG 1,65

9 Win32.Worm.Downadup.B 1,25

10 Trojan.Script.236197 1,08

AUTRES 52,85

Â« *Les exploitations des PDF deviennent de plus en plus frÃ©quentes. En effet, il s'avÃ¨re que les documents exportÃ©s en PDF sont de plus en plus utilisÃ©s et exportÃ©s avec des outils qui ne sont pas forcement de derniÃ¨re gÃ©nÃ©ration, ouvrant ainsi une porte aux exploits. Quant aux Autorun, un grand nombre des nouveaux codes malveillants utilisent cette technique permettant de vÃ©hiculer leurs codes facilement de rÃ©seaux en rÃ©seaux par le biais de clÃ©s USB et de disques durs. Il est clair que des techniques utilisÃ©es par de grands vers tels que Downadup ou mÃªme des vers SDBOT exploitant les failles RPC continueront d'infecter les rÃ©seaux, car pour y faire face, il s'agit de protÃ©ger la totalitÃ© des postes et serveurs en mÃªme temps...ce qui est parfois la grande difficultÃ© des entreprises aujourd'hui.* Â» dÃ©clare **Marc Blanchard**, Ã©pidÃ©miologiste et Directeur des Laboratoires Editions Profil pour BitDefender en France.

Pour Ãªtre informÃ© des derniÃ¨res e-menaces, inscrivez-vous aux **flux RSS BitDefender**