

Top 10 des mÃ©chants de juin selon BitDefender

SÃ©curitÃ©

PostÃ© par : JerryG

PubliÃ©e le : 8/7/2008 15:02:15

Le trojan Â« **Trojan.FakeAlert.PP** Â» gagne **une place dans le Top 10 du mois de juin publiÃ© par les laboratoires antimalware BitDefender.**

Son mode de fonctionnement est d'alerter les utilisateurs Ã propos de fausses infections qui toucheraient leurs ordinateurs et qui demandent une analyse antivirale avec un antivirus factice intitulÃ© Â« **XP antivirus** Â».



Ã

Son succÃ©s reste limitÃ©, comme le dÃ©montre le fait que XP antivirus, lui-mÃªme, ne soit pas dans le Top 10, mais il semble nÃ©anmoins profiter d'un large rÃ©seau de diffusion via des sites Web malveillants et corrompus.

Pas de changement depuis le dernier classement pour les deux premiÃ©res places, avec Trojan.clicker.CM et Trojan.Downloader.WMA.Wimad.N qui comptent toujours pour plus de **10 %** du nombre total de dÃ©tections. En gÃ©nÃ©ral, les trojans sont en position de force, puisqu'Ã©c'est la seule place de ce Top 10 des e-menaces n'est pas occupÃ©e par un cheval de Troie.

On retrouve **Exploit.SWF.Gen** Ã la sixiÃ©me place, qui reprÃ©sente une dÃ©tection gÃ©nÃ©rique pour une catÃ©gorie de fichiers .SWF (Flash) fabriquÃ©e spÃ©cifiquement. Le chargement de ce type de code permet l'Ã©xecution de fichiers Ã distance lorsque le client utilise une version de Flash player vulnÃ©rable.

Habituellement, ce type de menace utilise un shellcode qui en retour tÃ©lÃ©charge et exÃ©cute un trojan voleur de mots de passe.

Ã

Aux 8Ã¨me et 9Ã¨me places, se trouvent les fichiers dÃ© une variÃ©tÃ© de trojans utilisant une technique Ã©prouvÃ©e qui tire profit de la fonction âautorunâ de Microsoft Windows â sur les systÃ©mes dont lâautorun est activÃ© - en exÃ©cutant automatiquement un fichier intitulÃ© Autorun.inf lors de lâaccÃ©s Ã un rÃ©pertoire contenant ce fichier.

Ces trojans profitent de la faiblesse de cette caractÃ©ristique pour se propager via le partage de fichiers et de dossiers.