BitDefender Top 10 de novembre, L' exploitationt de la fonction Autorun
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 4/12/2009 0:00:00

La premiÃ¨re place du **Top 10 BitDefender du mois de novembre** est occupÃ©e par Trojan.AutorunInf.Gen, qui se trouvait en deuxiÃ¨me position dans le classement du mois dâ□□octobre. Il sâ□□agit dâ□□une famille gÃ©nÃ©rique de malwares exploitant la fonction Autorun (exÃ©cution automatique) des systÃ¨mes dâ□□exploitation Microsoft Windows.

Par dÃ©faut, tous les supports de stockage amovibles contiennent un script autorun.ini qui indique Ã lâ□□ordinateur quel fichier exÃ©cuter lorsque le support est connectÃ©. Les auteurs de malwares modifient souvent ce fichier afin de lui faire lancer diverses applications malveillantes.

Trojan.Clicker.CM perd une place et se retrouve deuxiÃ¨me de ce classement, avec presque 8% 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 de cÃ©lÃ¨bres logiciels commerciaux. Clicker.CM est utilisÃ© pour afficher des publicitÃ©s dans le navigateur de lâ□□utilisateur afin dâ□□obtenir un maximum de revenus par les publicitÃ©s.

La troisiÃ¨me position de ce rapport mensuel sur les menaces est occupÃ©e par **Win32.Worm.Downadup.Gen**. Ã□ lâ□□origine de presque 6% des infections, Win32.Worm.Downadup.Gen 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 limite 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 Downadup installent notamment de faux logiciels antivirus.

Trojan.Wimad occupe la quatriÃ¨me position avec 5% de lâ□□ensemble des infections. Il exploite la fonctionnalitÃ© permettant aux fichiers ASF de tÃ©lÃ©charger automatiquement les codecs appropriÃ©s Ã distance pour dÃ©ployer des fichiers binaires infectÃ©s sur lâ□□ordinateur hÃ´te.

Sous le nom dâ□□Exploit.PDF-JS.Gen 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 de binaires malveillants Ã distance. Cette menace correspond Ã 3,23% des infections totales.

Win32.Sality.OG, en sixiÃ¨me position avec 2,57% de lâ□□ensemble 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 de ce classement BitDefender du mois de novembre, 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 1,59% de lâ□□ensemble des infections.

Trojan.Inject.RA est un cheval de Troie voleur de mots de passe ciblant principalement les joueurs de Lineage II. Cette variante spÃ©cifique prÃ©sente un composant keylogger qui enregistre les frappes de clavier des utilisateurs et les envoie Ã un attaquant Ã distance via les protocoles HTTP ou SMTP.

Le classement sâ□□achÃ¨ve avec **Trojan.Downloader.Bredolab.AZ** qui reprÃ©sente 1,20% des systÃ¨mes infectÃ©s dans le monde. Le cheval de Troie se fait passer pour un document de Microsoft Word, injecte un fichier DLL et lâ□□enregistre en tant quâ□□objet dâ□□aide Ã la navigation. Trojan.Downloader.Bredolab.AZ surveille les frappes de clavier des utilisateurs via un composant keylogger et envoie les donnÃ©es recueillies Ã un site Internet en Russie.

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