Mercredi 13 janvier 2010

Exploit.PDF-JS.Gen met un terme à la domination des chevaux de Troie dans le top 10 BitDefender de décembre 2009

Un exploit PDF prend la tête du classement

La tête du classement du top 10 de ***BitDefender***® est occupée par l'e-menace Exploit.PDF-JS.Gen, qui représente 12,04% de l'ensemble des infections. Sous ce nom sont regroupés des fichiers PDF qui exploitent différentes vulnérabilités détectées dans le moteur Javascript de PDF Reader, afin d'exécuter du code malveillant sur l'ordinateur de l'utilisateur. Après l'ouverture d'un fichier PDF infecté, un code Javascript spécialement conçu à cet effet entraîne le téléchargement à distance de codes binaires malveillants.

Avec 8,15% des infections, la deuxième e-menace de ce Top 10 du mois de décembre 2009 est Trojan.AutorunInf.Gen, un mécanisme générique de diffusion de malwares via des périphériques amovibles tels que les clés USB, les cartes mémoire 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 troisième position ce mois-ci avec 7,90% des infections totales. On le trouve principalement sur des sites Internet proposant des applications illégales telles que des cracks, des keygens et des numéros de série des logiciels commerciaux les plus prisés. Ce cheval de Troie est utilisé principalement pour afficher des publicités dans le navigateur des utilisateurs afin d'obtenir un maximum de revenus par les publicités.

À l'origine de 5,85% des infections, Win32.Worm.Downadup.Gen occupe la quatrième position du classement de ce mois. Ce ver exploite une vulnérabilité du service serveur RPC de Microsoft Windows permettant l'exécution de code à distance (MS08-67) afin de se diffuser sur d'autres ordinateurs du réseau local. Il restreint également l'accès des utilisateurs à Windows Update et aux sites d'éditeurs de sécurité informatique. De nouvelles variantes du ver installent également de faux logiciels antivirus.

Trojan.Wimad.Gen.1 occupe la cinquième position avec 4,57% de l'ensemble des infections. Il exploite principalement la fonctionnalité permettant aux fichiers ASF de télécharger à distance les codecs appropriés pour déployer des fichiers binaires infectés sur l'ordinateur hôte. Le format ASF stocke des données aux formats WMA (Windows Media Audio) ou WMV (Windows Media Video), que l'on trouve principalement sur les sites Internet de torrents. En lecture locale, ce fichier WMV spécialement conçu tente de télécharger un « codec spécial » qui s'avère être un code binaire malveillant provenant d'un site tiers.

La sixième place, correspondant à 2,65% des infections mondiales, est occupée par Win32.Sality.OG. Cette e-menace malveillante est un infecteur de fichiers polymorphe qui ajoute son code crypté aux fichiers exécutables (binaires .exe et .scr). Afin de ne pas se faire remarquer, elle déploie un rootkit sur la machine infectée et supprime les applications antivirus en cours d'exécution sur l'ordinateur.

Trojan.Autorun.AET, en septième position avec 1,97% des infections totales, est un code malveillant qui se diffuse via les dossiers partagés de Windows et les supports de stockage amovibles. Ce cheval de Troie exploite la fonctionnalité Autorun des systèmes d'exploitation Windows pour lancer automatiquement des applications lorsqu'un support de stockage infecté est connecté.

Worm.Autorun.VHG est un ver de réseau/Internet qui exploite la vulnérabilité Windows MS08-067 afin de s'exécuter à distance en utilisant un package RPC (Remote Procedure Call) spécialement conçu à cet effet (une technique également utilisée par Win32.Worm.Downadup). Le ver est huitième du classement avec 1,65% de l'ensemble des infections.

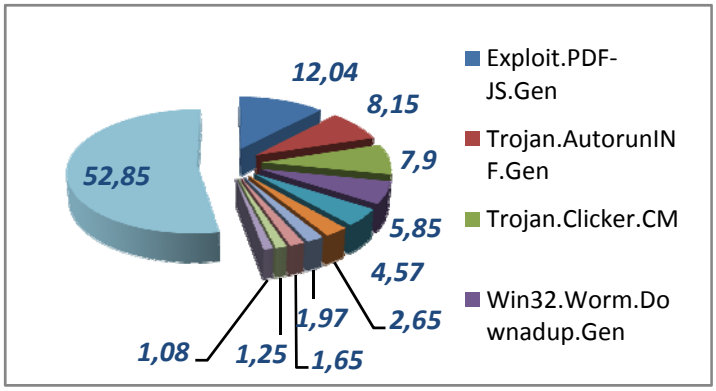
Win32.Worm.Downadup.B occupe la neuvième position du classement avec 1,08%. C'est une variante de Win32.Worm.Downadup avec pratiquement les mêmes fonctionnalités, si ce n'est que le

nombre d'URL de sites d'antivirus bloqués est inférieur. C'est également l'une des variantes les moins dangereuses, puisqu'elle n'a pas de charge utile malveillante.

Le Top 10 du mois de décembre 2009 s'achève avec Trojan.Script.236197. À l'origine de 1,08% des infections, ce fichier JavaScript « obscurci » affiche des fenêtres pop-up imitant les alertes MSN Messenger lorsque l'utilisateur visite un site Internet pour adultes. Les publicités, transmises via le service DoublePimp, ressemblent à une conversation en temps réel avec une femme censée se trouver dans la même zone géographique que le fournisseur d'accès de l'utilisateur.

Top 10 BitDefender des e-menaces du mois de décembre 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



« Les exploitations des PDF deviennent de plus en plus fréquentes. En effet, il s'avère que les documents exportés en PDF sont de plus en plus utilisés et exportés avec des outils qui ne sont pas forcement de dernière génération, ouvrant ainsi une porte aux exploits. Quant aux Autorun, un grand nombre des nouveaux codes malveillants utilisent cette technique permettant de véhiculer leurs codes facilement de réseaux en réseaux par le biais de clés USB et de disques durs. Il est clair que des techniques utilisées par de grands vers tels que Downadup ou même des vers SDBOT exploitant les failles RPC continueront d'infecter les réseaux, car pour y faire face, il s'agit de protéger la totalité des postes et serveurs en même temps...ce qui est parfois la grande difficulté des entreprises aujourd'hui. » déclare Marc Blanchard, épidémiologiste et Directeur des Laboratoires Editions Profil pour BitDefender en France

Pour être informé des dernières e-menaces, inscrivez-vous aux flux RSS BitDefender à l'adresse suivante : http://www.bitdefender.fr/site/Using-Rss-Feeds.html

À propos de BitDefender®

*BitDefender est la société créatrice de l'une des gammes de **solutions de sécurité** la plus complète et la plus certifiée au niveau international, reconnue comme étant parmi les plus rapides et les plus efficaces du marché. Depuis sa création en 2001, BitDefender n'a cessé d'élever le niveau et d'établir de nouveaux standards en matière de protection proactive des menaces. Chaque jour, BitDefender protège des dizaines de millions de particuliers et de professionnels à travers le monde – en leur garantissant une utilisation sereine et sécurisée de l'univers informatique. Les **solutions de sécurité** BitDefender sont distribuées dans plus de 100 pays via des partenaires revendeurs et distributeurs hautement qualifiés. Dans les pays francophones, BitDefender est édité en exclusivité par Éditions Profil. Plus d'informations sur BitDefender et ses solutions sont disponibles via le **Centre de presse**. Retrouvez également sur le site **www.malwarecity.fr** les dernières actualités au sujet des menaces de sécurité qui permettent aux utilisateurs de rester informés des dernières évolutions de la lutte contre les malwares.*

À propos des Editions Profil

Editions Profil, société indépendante créée en 1989, développe, édite et diffuse des logiciels sur différents secteurs d'activités, professionnel et grand public. L'éditeur a constitué un large catalogue de solutions dans de nombreux domaines, par exemple sur les segments de la bureautique et de la productivité. Editions Profil s'est plus particulièrement spécialisée ces dernières années dans l'édition et la distribution d'outils de sécurité informatique et la protection des données en général. Editions Profil édite notamment les solutions de sécurité BitDefender et de contrôle parental Parental Filter 2, ainsi que les solutions Farstone et diffuse les solutions de récupération de données et de gestion de serveurs MS Exchange de Kroll-Ontrack.