Le mercredi 4 novembre 2009

Les chevaux de Troie continuent à dominer le Top 10 BitDefender des e-menaces en octobre

Trojan.Clicker.CM conserve la première place

Trojan.Clicker.CM, présent principalement sur les sites Internet qui proposent des applications illégales telles que des cracks, des keygens et des numéros de série de logiciels commerciaux, occupe de nouveau, pour le mois d'octobre cette fois-ci, la première place du Top 10 BitDefender. Il est généralement utilisé pour afficher des publicités dans le navigateur et représente 9,47% des fichiers infectés en octobre.

Trojan.AutorunInf.Gen, qui occupe la deuxième place avec 8,54% des infections, est un mécanisme générique utilisé pour diffuser des malwares via des supports amovibles tels que des clés USB, des cartes mémoires ou des disques durs externes. Win32.Worm.Downadup et Win32.TDSS sont deux célèbres familles de malwares qui utilisent cette approche pour causer de nouvelles infections.

Win32.Worm.Downadup se trouve en troisième position avec 5,29% de l'ensemble des machines infectées. Aussi connu sous les noms de Conficker ou Kido, le ver bloque l'accès aux sites Internet de sécurité informatique. Mais la dernière version du ver va encore plus loin en installant de faux logiciels de sécurité sur les machines compromises.

En quatrième position, **Trojan.Wimad** représente 4,90% des infections**.** Il exploite une fonctionnalité moins connue mise en place par Microsoft afin de stocker des données multimédias synchronisées. Ce cheval de Troie affecte les fichiers ASF, un format d'extension qui prend en charge la distribution de données sur une grande variété de réseaux tout en restant adapté à la lecture locale. Un fichier ASF spécialement corrompu exploite la fonctionnalité qui permet d'installer des codecs appropriés pour installer à la place des chevaux de Troie.

Sous le nom d'**Exploit.PDF-JS.Gen**, en cinquième position, 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 de binaires malveillants à partir d'emplacements distants. Cette menace correspond à 4,84% des infections mondiales.

Win32.Sality.OG, en sixième position avec 2,31% de l'ensemble des infections, 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, il déploie un rootkit sur la machine infectée et tente de supprimer les applications antivirus installées en local.

Trojan.Autorun.AET, en septième position avec 2,20% 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 1,49% de l'ensemble des infections.

Trojan.Swizzor.6 est une variante de la famille Swizzor, des téléchargeurs « cryptés » qui tentent d'enregistrer et d'exécuter de nouvelles menaces sur les machines infectées. Le cheval de Troie ajoute sa clé au Registre Windows afin d'exécuter une copie de lui-même à chaque fois que Windows est lancé. Cette variante spécifique de Swizzor représente 1,22% des infections mondiales.

Enfin, la dernière place du classement est occupée par **Gen:Adware.Heur.wq0@j4oukhei**, qui représente 1,21% de l'ensemble des infections. Cette signature générique détecte une large gamme d'applications adwares, dont la famille NaviPromo.

Top 10 BitDefender des e-menaces du mois d'octobre :

1	Trojan.Clicker.CM	9,47%
2	Trojan.AutorunINF.Gen	8,54%
3	Win32.Worm.Downadup.Gen	5,29%
4	Trojan.Wimad.Gen.1	4,90%
5	Exploit.PDF-JS.Gen	4,84%
6	Win32.Sality.OG	2,31%
7	Trojan.Autorun.AET	2,20%
8	Worm.Autorun.VHG	1,49%
9	Trojan.Swizzor.6	1,22%
10	Gen:Adware.Heur.wq0@j4oukhei	1,21%
	AUTRES	58,53%

Pour être informé des dernières e-menaces, inscrivez-vous aux flux RSS BitDefender ici.

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.