Le mardi 7 juillet 2009

Les chevaux de Troie dominent les e-menaces de juin

La suprématie de Conficker est en déclin alors que Trojan.Clicker.CM prend la tête du classement en contournant les bloqueurs de pop-up

BitDefender a publié la liste des dix principales e-menaces détectées en juin, et les chevaux de Troie continuent à dominer le classement : cinq des dix principales e-menaces sont des chevaux de Troie.

La dixième position est occupée par des e-menaces empaquetées avec **NSanti,** un programme très utilisé par les créateurs de virus pour tenter de masquer le contenu de leurs fichiers infectés et de réduire leur taille.

En neuvième position, **NaviPromo**, un ancien adware, qui a retrouvé un second souffle. NaviPromo est la « part obscure » de Navi, la tristement célèbre barre d'outils.

En huitième position, **Trojan.Autorun.AET** a utilisé ce qui est assurément devenu la « vulnérabilité de l'année » : le bug de l'Autorun de Windows, pour représenter 2,08% du nombre total de machines infectées.

La seule nouvelle e-menace de ce classement est **Trojan.Skintrim.HTML.A**, qui se fait passer pour un add-in d'Outlook appelé MailSkinner. Ce cheval de Troie associe en fait rootkit et backdoor pour tenter de télécharger et d'installer d'autres malwares sur les machines infectées.

Win32.Sality.OG, un infecteur de fichier qui installe un rootkit, gagne trois places depuis le mois de mai et occupe désormais la sixième position. Il est précédé de **Downadup.Gen,** aussi connu sous le nom de **Conficker** ou **Kido**. Cette e-menace est en léger recul, représentant 3,33% de l'ensemble des e-menaces en juin contre 4,35% le mois dernier.

Un exploit **SWF** largement utilisé se trouve en quatrième place. Bien qu'ancien, il doit probablement sa position aux nombreux virus qui l'incluent toujours à leur « arsenal ».

Trojan.Wimad, avec ses différentes variantes, occupe la troisième place. C'est un retour inattendu pour ce ver qui ne figurait pas dans le classement du mois dernier.

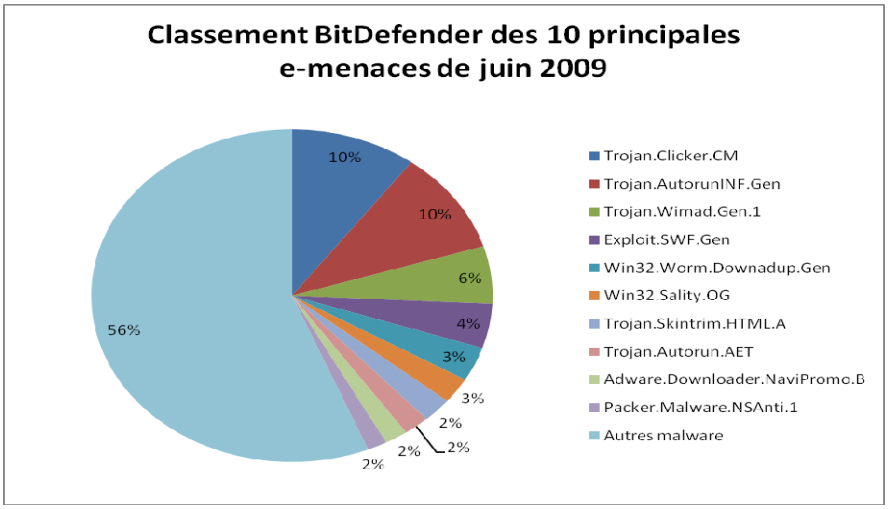
En seconde position, **Trojan.AutorunINF.Gen**, est une « famille » de malwares largement répandue qui utilise le fichier Autorun dans des dossiers partagés et des disques amovibles pour se diffuser. Cette e-menace est également en léger recul comparé au mois dernier et a été « détrônée » de la première place par **Trojan.Clicker.CM**, un simple adware se diffusant via des sites Web malveillants. Clicker est l'une des e-menaces les plus fréquentes cette année, et doit son « succès » à sa capacité à contourner les bloqueurs de pop-up.

Marc Blanchard, Directeur des Laboratoires BitDefender en France, ajoute : « Depuis quelques mois, nous rencontrons un nombre croissant d'infections actives qui transforment les ordinateurs des internautes en machines dites « zombies », qui sont pilotées à distance par des pirates, avec des attaques mutantes ou changeantes. Ces machines sont corrompues par de simples visites sur des sites web conventionnels qui ont été infectés. L'internaute n'a plus à effectuer des téléchargements spécifiques, une simple visite sur un site Web suffit pour subir une infection.
Les infections des autoruns sont également un vecteur de propagation important qu'il ne faut pas négliger, car un simple échange de clefs USB suffit à infecter un ordinateur et un réseau sur lequel l'ordinateur est connecté.
Concernant **Downadup**, de nombreuses entreprises continuent de se faire infecter, car elles n'ont pas encore appliqué les hotfixs proposés par Microsoft. Par conséquent, l'antivirus bloque ce ver à son

arrivée, mais le ver continuera d'effectuer des tentatives d'infections tant que la machine sur laquelle le ver fonctionne ne sera pas patchée. A noter que les ordinateurs patchés, avec un antivirus à jour, mais continuant de détecter cette e-menace ne sont plus vulnérables aux versions actuelles de Confiker. »

Classement BitDefender des 10 principales e-menaces de juin 2009 :

Pos	Nom	%
1.	Trojan.Clicker.CM	10.13
2.	Trojan.AutorunINF.Gen	10.04
3.	Trojan.Wimad.Gen.1	5.6
4.	Exploit.SWF.Gen	4.34
5.	Win32.Worm.Downadup.Gen	3.33
6.	Win32.Sality.OG	2.5
7.	Trojan.Skintrim.HTML.A	2.37
8.	Trojan.Autorun.AET	2.08
9.	Adware.Downloader.NaviPromo.B	1.84
10.	Packer.Malware.NSAnti.1	1.59
	Autres malware	**56.18**



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 reconnues 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 Parental Filter, ainsi que les solutions Farstone et diffuse les solutions de récupération de données et de gestion de serveurs MS Exchange de Kroll-Ontrack.