Le vendredi 29 mai 2009

TOP 10 BitDefender des e-menaces de mai 2009

Les Chevaux de Troie continuent à dominer le top 10 des e-menaces en mai

La technique d'infection utilisant le code d'exécution automatique des programmes : autorun.inf se place en tête du classement.

BitDefender a publié aujourd'hui la liste des dix principales e-menaces détectées en mai. Comme au mois d'avril , ce sont les chevaux de Troie qui figurent principalement en tête de ce classement. Les malwares nécessitant l'interaction des utilisateurs, occupent six positions sur dix, dont les trois premières places.

Trojan.JS.PYV fait son apparition dans le classement en dixième position, avec 1,73% des détections, précédé de Trojan.Autorun.AET (en 9ème position), un cheval de Troie se diffusant également via des dossiers partagés, exploitant l'Autorun : la fonction d'exécution automatique des programmes de Windows.

Storm Worm, 7ème du classement, fait son retour, cette fois-ci comme composant « déposé» c'est-à-dire qu'il ne se propage pas par lui-même, mais est installé par l'intermédiaire d'une autre e-menace, sans doute pour servir de « contrôle à distance » sur l'ordinateur infecté.

Un infecteur de fichiers polymorphes se trouve en 6ème position ce mois-ci, et s'il paraît dangereux, il l'est effectivement : le virus infecte des fichiers exécutables ainsi que des partages réseau, se réécrivant durant le processus afin d'éviter la détection par des analyses basées sur les signatures.

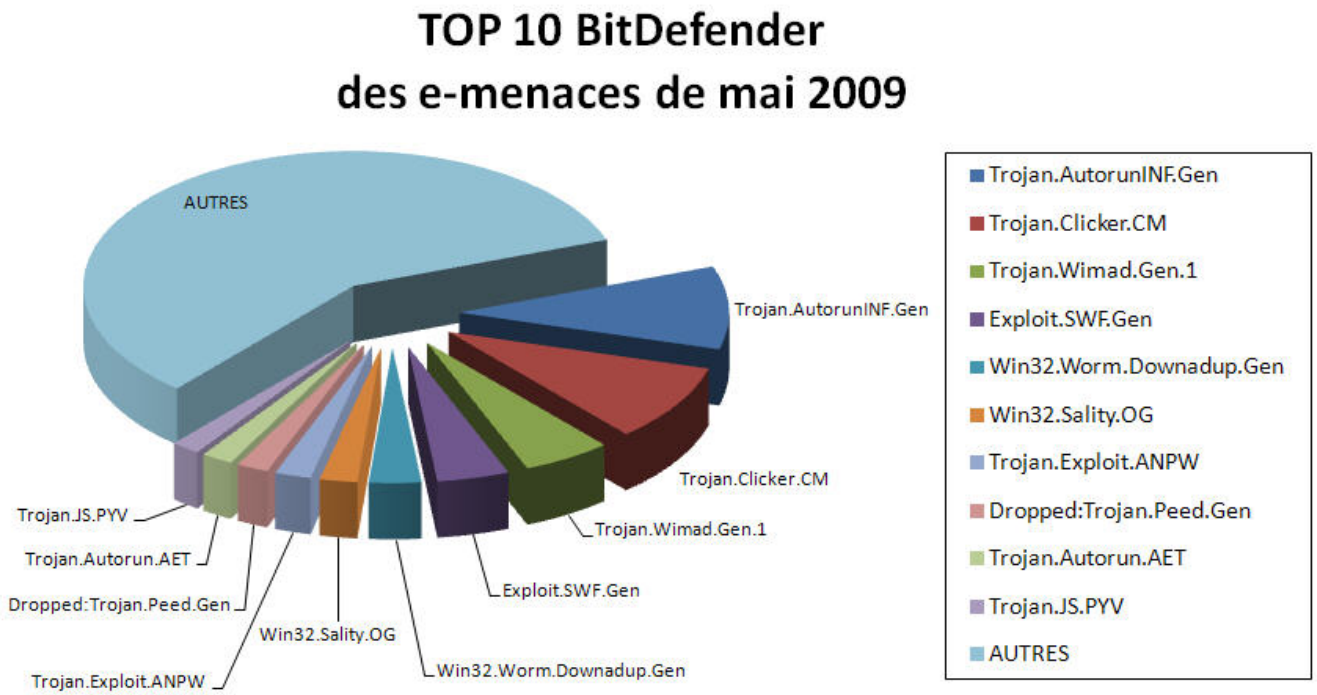
Une fois qu'un fichier infecté de ce type est exécuté directement, ou lorsque le partage dans lequel il se trouve est ouvert et que l'option « Autorun » est activée, le virus installe un rootkit sur l'ordinateur. Le rootkit permet à l'attaquant un contrôle total sur le PC infecté, alors que le virus en lui-même, agit ensuite comme un scanneur de ports essayant de trouver des services UDP ouverts sur des ordinateurs choisis de manière aléatoire.

Conficker progresse toujours, pour parvenir à la cinquième position ce mois-ci, représentant 3,12% des infections détectées, alors qu'un petit morceau de code de l'exploit SWF, très utilisé dans les sites malveillants et corrompus du monde entier, se retrouve en quatrième position, avec 4,33%.

En troisième position, le cheval de Troie Wimad, une e-menace se faisant passer pour un lecteur vidéo, est le premier à dépasser la barre des 5% (il représente 5,34% des détections).

Le très ancien Trojan.Clicker.CM, un programme affichant des fenêtres pop-up, occupe la deuxième place avec 9,23% des détections.

Enfin, la première place de ce classement n'est pas occupée par un malware, mais plutôt par une technique d'infection : le code d'exploitation autorun.inf, détecté dans des menaces aussi diverses que Conficker et Sality, correspond à 9,93% des détections, ce qui en fait l'exploit le plus répandu au monde et le premier de notre classement mensuel.



1.	Trojan.AutorunINF.Gen	9,93
2.	Trojan.Clicker.CM	9.23
3.	Trojan.Wimad.Gen.1	5,34
4.	Exploit.SWF.Gen	4,33
5.	Win32.Worm.Downadup.Gen	3,12
6.	Win32.Sality.OG	2,25
7.	Trojan.Exploit.ANPW	2,17
8.	Dropped:Trojan.Peed.Gen	1,9
9.	Trojan.Autorun.AET	1,87
10.	Trojan.JS.PYV	1,73
	Autres malwares	**58.13**

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.