

Top 10 BitDefender des e-menaces du mois de février 2010

Sécurité

Posté par : JerryG

Publié le : 2/3/2010 0:00:00

Les périphériques amovibles sont les principaux vecteurs de diffusion des malwares ce mois-ci

Avec 2 chevaux de Troie, 2 exploits et 1 ver en tête de ce classement des e-menaces, la composition des malwares a quelque peu changé, les exploits étant plus présents en février.

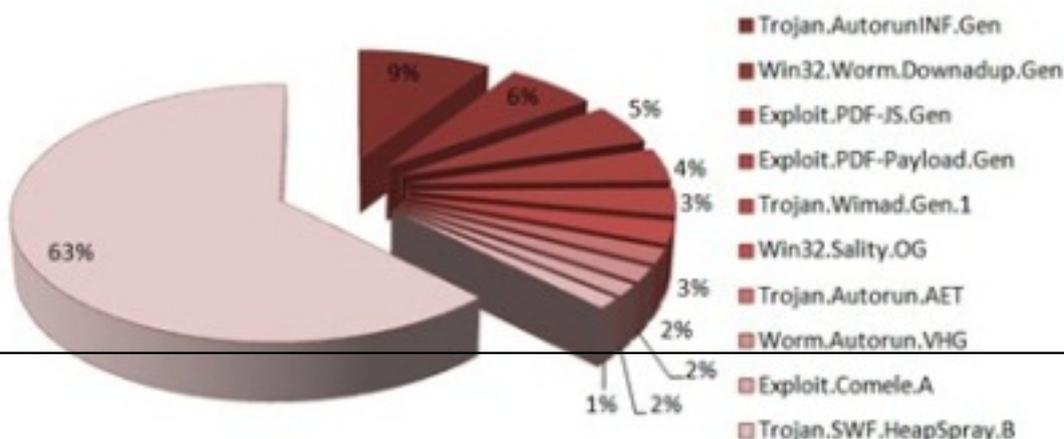
Le mois de février nous a réservé une surprise. Le malware en tête du classement du mois dernier (Trojan.Clicker.CM) a complètement disparu du panorama actuel.



La première position du top 10 est désormais détenue par **Trojan.AutorunInf.Gen**, un mécanisme générique de diffusion de malwares via des périphériques amovibles tels que des clés USB, des cartes mémoire ou des disques durs externes, qui correspond à 9,09% de l'ensemble des malwares.

Catalan Cosoi, chercheur chez BitDefender® rappelle que « les périphériques externes devraient être analysés rigoureusement » avant d'ajouter qu'« il s'agit d'une mesure de sécurité destinée particulièrement aux périphériques ayant été utilisés dans des bibliothèques, des cybercafés et d'autres lieux publics connus pour être des sources d'infection ».

Le top 10 BitDefender des malwares du mois de février 2010:



Win32.Worm.Downadup.Gen a progressé d'une place par rapport au mois de janvier. En deuxième position, avec 6,24% des infections totales, ce ver exploite une vulnérabilité de Microsoft® Windows® bien connue. « La présence constante de ce ver dans nos classements mensuels sur les malwares révèle la réticence de la plupart des utilisateurs à mettre à jour leur système d'exploitation et leur solution antimalware installée en local, ainsi qu'à installer des correctifs de sécurité publiés par Microsoft® il y a plus d'un an maintenant », explique **Catalin Cosoi**, chercheur chez BitDefender®. De nouvelles variantes de ce ver installent également de faux logiciels antivirus.

Récapitulatif du top 10 BitDefender des e-menaces du mois de février 2010 :

1	Trojan.AutorunNF.Gen	9,09%
2	Win32.Worm.Downadup.Gen	6,24%
3	Exploit.PDF-JS.Gen	5,13%
4	Exploit.PDF-Payload.Gen	4,21%
5	Trojan.Wimad.Gen.1	3,37%
6	Win32.Sality.OG	2,77%
7	Trojan.Autorun.AET	1,92%
8	Worm.Autorun.VHG	1,85%
9	Exploit.Comele.A	1,48%
10	Trojan.SWF.HeapSpray.B	1,40%
	AUTRES	62,53%

En troisième et en quatrième position de ce classement de février, **Exploit.PDF-JS.Gen** et **Exploit.PDF-Payload.Gen** correspondent respectivement à 5,13% et 4,21 % des infections totales. Sous ces noms sont regroupés des fichiers PDF manipulés exploitant différentes vulnérabilités détectées dans le moteur Javascript d'Adobe® PDF Reader® afin d'exécuter du code malveillant sur les ordinateurs des utilisateurs.

Les torrents continuent à faire partie des vecteurs de diffusion favoris. Avec 3,37%, Trojan.Wimad.Gen.1 clôture ce top 5 en conservant la position qui était la sienne au mois de janvier. Il pourrait bien apparaître sous la forme d'un épisode inédit de votre série TV préférée ou d'un film succès.