Les chevaux de Troie dominent encore le Top 10 BitDefender en avril
SÃ©curitÃ©
PostÃ© par : JerryG
PubliÃ©e le : 8/5/2009 0:00:00

Bien que Conficker soit encore bien prÃ©sent dans la liste, **d'autres e-menaces commencent Ã utiliser des mÃ©thodes similaires pour se propager**
BitDefender publie aujourd'hui la liste des dix menaces les plus dangereuses pour les utilisateurs d'Internet au cours du mois d'avril. Ã l'instar du mois de mars, le sommet du classement est toujours dominÃ© par les chevaux de Troie.

Ces menaces, dont le mode de fonctionnement est de piÃ©ger les utilisateurs pour accÃ©lÃ©rer leur propagation, occupent sept des dix premiÃ¨res places du classement de ce mois-ci.

Top 10 BitDefender des principales e-menaces d'avril 2009

Pos.	Nom	%
1.	Trojan.AutorunINF.Gen	9,0
2.	Trojan.Clicker.CM	8,47
3.	Trojan.Wimad.Gen.1	5,68
4.	Win32.Worm.Downadup.Gen	3,05
5.	Trojan.Exploit.ANPW	2,84
6.	Exploit.SWF.Gen	2,4
7.	Win32.Sality.OG	2,1
8.	Trojan.KillAV.PT	1,91
9.	Dropped:Trojan.Peed.Gen	1,81
10.	Trojan.Exploit.SSX	1,74
	Autres malwares	**60,99**

Â

Â

Trojan.Peed.Gen (alias le redoutable Â« Storm Worm Â») reprÃ©sente 1,81 % des dÃ©tections du mois d'avril, mais c'est dÃ©sormais un composant "dropper", c'est-Ã -dire qu'il dÃ©pose des virus au profit d'une menace diffÃ©rente. Cela indique que, bien qu'il soit toujours utilisÃ©, l'efficacitÃ© de ce ver en tant que virus infectieux est rÃ©volue et qu'il est dÃ©sormais utilisÃ© uniquement pour la fonctionnalitÃ© de contrÃ´le qu'il fournit aux cyber-attaquants.

Un nouveau venu se place en huitiÃ¨me position : Trojan.KillAV.PT.

Cette menace est un logiciel malveillant "utilitaire" qui dÃ©truit tous les antivirus ou processus de sÃ©curitÃ© (parmi une longue liste) qu'il peut trouver sur un ordinateur cible afin d'empÃªcher leur exÃ©cution. Ensuite, la menace dÃ©crypte et exÃ©cute un tÃ©lÃ©chargeur qui, Ã son tour, tÃ©lÃ©charge et installe un programme permettant de dÃ©rober les mots de passe utilisÃ© dans des jeux.

Ã la septiÃ¨me place, **Win32.Sality** est le seul virus vÃ©ritable du top 10 du mois d'avril. Win32.Sality est un virus polymorphe qui infecte les fichiers exÃ©cutables (.exe et .src) en les modifiant et en ajoutant son corps cryptÃ© dans une nouvelle section, Ã la fin de ces derniers.

Ses autres moyens de diffusion consistent en une nouvelle (bien quâancienne) mÃ©thode : se combiner Ã un exÃ©cutable infectÃ© dans le fichier Autorun.INF qui se trouve sur un mÃ©dia amovible ou des partages de rÃ©seau, une technique utilisÃ©e plus rÃ©cemment par le ver Downadup / Conficker.