

Rapport trimestriel de PandaLabs (janvier – mars 2009)

Le nombre de nouveaux logiciels espions a connu une croissance de 10 % au premier trimestre 2009

- Le spyware Virtumonde est le code malveillant qui a infecté le plus d'ordinateurs.
- Les chevaux de Troie et les adwares sont toujours les types de malwares les plus répandus.
- Le ver Conficker est la menace qui a le plus mobilisé les laboratoires antivirus.
- Le rapport trimestriel de PandaLabs peut être téléchargé à l'adresse : <http://www.pandasecurity.com/homeusers/security-info/tools/reports.htm>

Paris, le 16 avril 2009

PandaLabs, le laboratoire de détection et d'analyse des malwares de Panda Security, présente son rapport sur les menaces du premier trimestre 2009 (<http://www.pandasecurity.com/homeusers/security-info/tools/reports/>). D'après ce rapport, les chevaux de Troie ont représenté 73 % de tous les nouveaux malwares créés pendant cette période. Cependant, une des principales menaces identifiées dans ce rapport est l'essor des spywares. Les logiciels espions ont connu une croissance de 2,5 % par rapport au trimestre précédent, atteignant 13,15 % de l'ensemble des menaces.

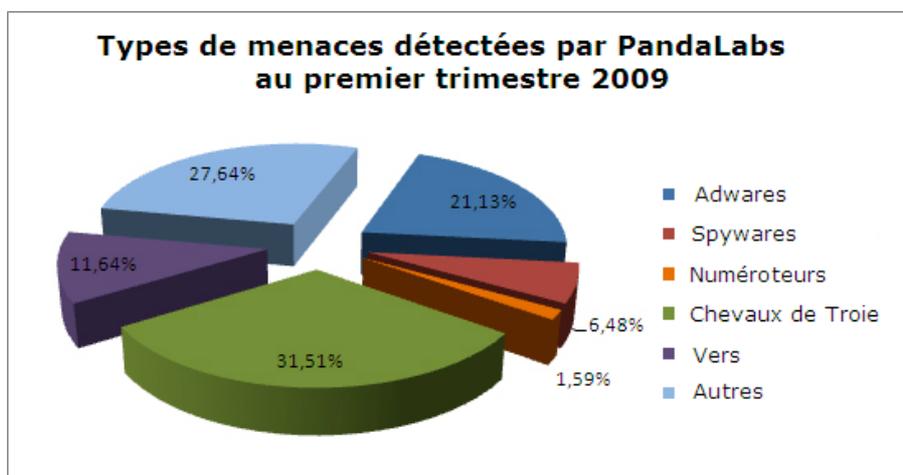
« Nous avons constaté une hausse considérable du nombre de logiciels espions en circulation au premier trimestre de l'année. L'objectif est probablement de saturer les laboratoires antivirus afin d'infecter davantage d'utilisateurs. », indique Luis Corrons, le directeur technique de PandaLabs.

Dans certains cas, la stratégie des cybercriminels a payé, comme avec le logiciel espion Virtumonde. Celui-ci a infecté plus d'ordinateurs qu'aucun autre code malveillant au premier trimestre 2009. Ce malware combine des fonctions d'adware et de spyware : il surveille l'activité des utilisateurs sur Internet, modifie les résultats sur les moteurs de recherche et affiche des bannières publicitaires et des pop-ups pour certains produits.

Malwares à l'origine du plus grand nombre d'infections

01	Spyware/Virtumonde
02	Trj/Rebooter.J
03	Adware/Yassist
04	Adware/Antivirus2009
05	W32/Bagle.RP.worm
06	Adware/AccesMembre
07	W32/Bagle.RC.worm
08	W32/Conficker.C.worm
09	W32/AutoRun.DJ.worm
10	W32/Gamania.gen

Malgré la hausse notable des spywares, ce sont toujours les chevaux de Troie (31,51 %) et les adwares (21,13 %) qui sont les premiers au niveau du nombre d'infections sur les trois premiers mois de l'année.



Taiwan est encore le pays où le pourcentage de malwares actifs est le plus élevé (31,7 %). Le Brésil et la Turquie sont également en bonne place. Ils sont, respectivement, à la deuxième et la troisième place des pays les plus infectés par des malwares actifs, devant l'Espagne et les États-Unis. Le Mexique a connu une baisse d'environ 10 % des infections de codes actifs, passant de 24,87 % en 2008 à 17,95 %.

Conficker, la principale menace du premier trimestre

Bien que cette menace soit apparue à la fin de l'année 2008, le ver Conficker est le code malveillant qui a le plus mobilisé les efforts des éditeurs de solutions de sécurité pendant les trois premiers mois de l'année, en raison du grand nombre d'infections intervenues entre décembre 2008 et janvier 2009.

La réactivation du ver, attendue pour le mois d'avril 2009, a suscité beaucoup d'inquiétudes. Cependant, jusqu'à présent, aucune nouvelle version ou infection n'a été détectée hormis celles des variantes précédentes déjà actives.

« Les nouvelles adresses ajoutées par le ver Conficker peuvent à tout moment être activées pour télécharger une mise à jour du code malveillant ou de nouveaux malwares. Dans tous les cas, cette menace ne concerne que les utilisateurs, encore trop nombreux, qui sont sans protection contre Conficker. », indique Luis Corrons.

Le rapport trimestriel de PandaLabs inclut également des informations sur d'autres sujets tels que le ver Waledac qui a fait parler de lui lors de la Saint Valentin, les malwares sur les réseaux sociaux ou les vulnérabilités les plus importantes des trois premiers mois de l'année. Vous pouvez télécharger le rapport (en anglais) à l'adresse : <http://www.pandasecurity.com/homeusers/security-info/tools/reports/>.

A propos de PandaLabs

Depuis 1990, la mission de PandaLabs est d'analyser les nouvelles menaces le plus rapidement possible pour assurer une totale sécurité à nos clients. Pour cela, PandaLabs a développé un système automatisé et innovant qui analyse et traite les milliers de nouveaux échantillons reçus chaque jour et renvoie automatiquement un verdict (logiciel malveillant ou inoffensif). Ce système repose sur l'Intelligence Collective Antimalware, le nouveau modèle de sécurité de Panda Security, qui détecte même les codes malveillants capables de passer au travers des autres solutions de sécurité.

Actuellement, 94 % des malwares détectés par PandaLabs sont analysés par l'Intelligence Collective Antimalware. Cette analyse automatique est complétée par le travail de plusieurs équipes spécialisées dans chaque type spécifique de malware (virus, vers, chevaux de Troie, logiciels espions, phishing, spam, rootkits, etc.) qui travaillent 24 heures sur 24 et 7 jours sur 7 pour offrir une garantie maximale. Grâce à ce système, Panda peut offrir à ses clients des solutions plus sûres, plus simples et consommant moins de ressources.

Pour plus d'informations, visitez le blog de PandaLabs : <http://www.pandalabs.com>

Pour plus d'informations :
communication@pandasecurity.com
Tel. +34 91 806 37 00

	<p>ATTACHÉE DE PRESSE : ÉMILIE SACKSICK SACKSICK@ELIOTROPE.FR ☎ LIGNE DIRECTE : 01 53 17 16 43</p>	<p>ELIOTROPE 151, rue du Faubourg Saint Antoine 75011 Paris France www.eliotrope.fr TEL : + 33 (0)1 53 17 16 40 FAX : + 33 (0)1 53 17 16 41</p>
---	--	--