

## Rapport hebdomadaire Panda Software sur les virus et les intrusions

Poissy, le 17 juillet 2006

Le rapport de PandaLabs s'intéresse cette semaine au cheval de Troie **Trj/Semsys.B**, au programme potentiellement indésirable **SpyHeal** et aux sept vulnérabilités publiées par Microsoft : **MS06-033**, **MS06-034**, **MS06-035**, **MS06-036**, **MS06-037**, **MS06-038** et **MS06-039**.

**Trj/Semsys.B** est un cheval de Troie qui utilise MSN Messenger pour envoyer des messages contenant un lien malicieux. Lorsque l'utilisateur clique sur ce lien, il télécharge involontairement un cheval de Troie banker. Il installe également un composant destiné à dérober les mots de passe des utilisateurs de la communauté Orkut, qui sont alors envoyés au pirate par e-mail.

**SpyHeal** est un programme potentiellement indésirable (PUP) qui vérifie la présence de menaces possibles dans le système sur lequel il est installé. Lorsqu'il en découvre, il informe l'utilisateur qu'un malware est présent sur son ordinateur et lui demande d'acheter un certain programme de sécurité. Toutefois, les menaces qu'il détecte ne sont pas réelles. En parallèle, il crée une entrée de registre pour s'assurer d'être exécuté à chaque démarrage du système d'exploitation. **SpyHeal** peut être téléchargé sur le site web de l'entreprise qui l'a développé.

Microsoft a publié dernièrement une série de bulletins de sécurité affectant plusieurs de ses produits.

**MS06-033** est une vulnérabilité importante de Microsoft.NET Framework 2.0 qui permet à un pirate de détourner la protection ASP.Net et d'obtenir un accès non autorisé à des objets du dossier de l'application.

**MS06-034** concerne une vulnérabilité importante de plusieurs versions de IIS (Internet Information Services) qui peut permettre à un pirate de prendre le contrôle de l'ordinateur avec les mêmes droits que ceux de l'utilisateur actif. Un fichier ASP spécialement conçu est nécessaire pour exploiter la vulnérabilité.

**MS06-035** est un ensemble de vulnérabilités critiques du service serveur de Windows 2003/XP/2000 qui peut permettre d'exécuter à distance du code arbitraire sur l'ordinateur et de donner l'accès à des informations sur le protocole SMB. L'utilisation d'un firewall peut prévenir l'exploitation de ces vulnérabilités.

**MS06-036** est une vulnérabilité critique du service client DHCP qui peut être exploitée pour exécuter du code avec les mêmes autorisations que l'utilisateur actif. Pour que l'attaque réussisse, le pirate doit envoyer à l'hôte infecté une réponse DHCP spécialement conçue depuis le même sous réseau. L'utilisation d'un firewall permet de se protéger contre ce type d'attaque lancée depuis Internet.

**MS06-037**, **MS06-038** et **MS06-039** sont un ensemble de vulnérabilités critiques découvertes dans plusieurs versions de Microsoft Office pour Windows et Mac, qui peuvent être exploitées pour permettre au pirate d'exécuter du code arbitraire sur le système affecté. Si l'utilisateur a les droits administrateurs, la vulnérabilité peut permettre au pirate de prendre le contrôle total de l'ordinateur.

Pour se prémunir des effets potentiels de ces vulnérabilités, nous conseillons de télécharger ces patches de sécurité, d'installer une solution antimalware et de la maintenir à jour.

Pour plus d'informations sur ces menaces ou sur toute autre menace, consultez [l'Encyclopédie de Panda Software](#)

Pour plus d'informations sur l'entreprise :

[http://www.pandasoftware.com/about\\_panda/companyprofile/15years.asp](http://www.pandasoftware.com/about_panda/companyprofile/15years.asp)

### **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. Plusieurs équipes, spécialisées dans chaque type spécifique de malware (virus, vers, chevaux de Troie, logiciels espions, phishing, spam, etc.) travaillent 24 heures sur 24 et 7 jours sur 7 pour offrir une garantie maximale. Pour cela, elles s'appuient sur les Technologies TruPrevent™, un véritable système global d'alertes, basé sur des sondes distribuées stratégiquement et qui permettent de neutraliser les nouvelles menaces et de les envoyer au plus tôt à PandaLabs pour les analyser. Selon Av.Test.org, PandaLabs est le laboratoire de virus qui offre les mises à jour complètes dans les délais les plus brefs. Plus d'informations à l'adresse : <http://www.pandasoftware.com/pandalabs.asp>.

Pour plus d'informations : [http://www.pandasoftware.com/virus\\_info](http://www.pandasoftware.com/virus_info)

### **Pour plus d'informations :**

Panda Software  
Département presse  
[communication@pandasoftware.com](mailto:communication@pandasoftware.com)

Tel: 01.30.06.15.15

Fax: 01.30.06.15.17