La Chine reste championne de l'hébergement de code malveillant

Sophos a identifié en mai 9.500 nouvelles pages Web infectées par jour, soit plus de 1.000 de plus qu'en avril, représentant un total de 304.000 sur l'ensemble du mois.

« Les attaques menées à partir du Web deviennent de mois en mois plus fréquentes et plus gênantes pour les entreprises », commente Michel Lanaspèze, Directeur Marketing et Communication de Sophos France et Europe du Sud. *« Rappelons que les sites de pirates n'ont pas besoin d'héberger de programmes malveillants pour être dangereux : nous détectons et bloquons également l'accès à plus de 600 nouvelles pages de phishing par jour. »*

« Les entreprises ne peuvent plus se contenter de filtrer les accès aux sites Web par catégories, les attaques les plus dangereuses se dissimulant désormais le plus souvent sur des pages légitimes », poursuit Michel Lanaspèze. *» C'est pourquoi les propriétaires de sites Web doivent impérativement disposer d'une sécurité adéquate et appliquer rigoureusement les correctifs nécessaires dès leur publication. »*

La liste des dix principales menaces issues du Web en mai 2007 est la suivante :1. Mal/Iframe 65.5% 2. JS/EncIFra 6.9% 3. Troj/Decdec 6.5% 4. Troj/Fujif 3.7% 5. Troj/Ifradv 3.0% 6. VBS/Redlof 2.2% 7. Mal/ObfJS 1.8% 8. Troj/Psyme 1.2% 9. VBS/Roor 1.0% 10. VBS/Soraci 0.9%Autres : 7,3%

Iframe, qui agit en introduisant du code malveillant à l'intérieur de pages web légitimes, continue à dominer le classement, avec près des deux tiers des menaces détectées en mai. Les trois nouveaux entrants, Redlof, Roor et Soraci, sont tous des virus ?parasites' qui infectent, entre autres, les fichiers HTM, HTML et HTT. L'apparition dans le Top Ten de ces virus relativement anciens montre que de nombreux administrateurs Web négligent de protéger efficacement leurs sites contre les pirates qui tentent de les compromettre à leur profit.

Le classement des dix principaux pays hébergeant des programmes malicieux en mai 20071. Chine (dont Hong Kong) 53.2% 2. Etats Unis 27.4% 3. Allemagne 5.1% 4. Russie 3.5% 5. Thaïlande 1.1% 6. Ukraine 1.0% 7. Royaume Uni 0.9% 8. Taiwan 0.8% 9. Canada 0.6% 10. Corée du Sud 0.5%Autres pays : 5,9%

La Chine, qui est responsable à elle seule de plus de 50% des pages web infectées identifiées par Sophos, conserve logiquement la première place du classement. Cette domination persistante est largement due à la diffusion croissante de Iframe, dont la présence a été repérée sur de nombreuses pages non protégées hébergées dans ce pays.

A noter que, **la France disparaît du classement**, la Thaïlande y apparaît pour la première fois en prenant directement la cinquième place. Les analyses de Sophos montrent qu'une proportion importante des pages infectées dans ce pays se trouvent sur des sites gouvernementaux.

« Le fait de trouver des programmes malveillants sur des sites Web officiels montre à nouveau qu'aucune organisation n'est à l'abri si elle n'est pas vigilante », conclut Michel Lanaspèze. *« Les utilisateurs du Web doivent eux aussi être prudents, car ce sont eux qui sont visés par ces sites. Ils doivent en particulier se méfier des messages de spam qui les incitent à cliquer sur les liens qui leur sont proposés, même lorsqu'ils paraissent*

authentiques, sans oublier de tenir à jour leur antivirus et leurs correctifs de sécurité ni de signaler à leur administrateur ou à leur FAI les sites infectés à bloquer. »

Classement des malwares diffusés via les messageries pour mai 2007:1. W32/Sober 29.0% 2. W32/Netsky 26.9% 3. W32/Mytob 13.1% 4. W32/Stratio 6.1% 5. W32/MyDoom 4.1% 6. W32/Zafi 3.9% =7. Mal/Behav 3.8% =7. W32/Sality 3.8% 9. W32/Bagle 3.3% 10. W32/Nyxem 1.8% Autres : 4.2%