

**Objet :** Propagation d'un nouveau cheval de Troie nommé Troj/Haxdoor-IN par courrier électronique. Le message invite les amateurs de football à télécharger gratuitement la calendrier des matchs pour suivre leurs équipes préférées. Installé par le destinataire, le cheval de Troie ouvre une brèche de sécurité permettant ainsi de contrôler à distance la machine victime.

**Systèmes concernés :** Windows 98, ME, NT, 2000, XP, Server 2003

|                                    |   |
|------------------------------------|---|
| <b>Effets</b>                      | <p>Une fois activé, le cheval de Troie <u>Troj/Haxdoor-IN</u> tente de :</p> <ul style="list-style-type: none"> <li>- ouvrir un port aléatoire pour permettre à des utilisateurs malveillants d'accéder à distance à la machine victime</li> <li>- désactive le firewall windows pour continuer à exécuter ses actions malveillantes</li> <li>- télécharger du code malveillant à partir de l'internet</li> <li>- s'installer dans le registre, ajoute, modifie et supprime des clés afin d'atténuer les paramètres de sécurité.</li> <li>- rendre certains fichiers cachés</li> </ul>  |
| <b>Signes visibles d'infection</b> | <ul style="list-style-type: none"> <li>- Lors de son exécution ,le troyen supprime du dossier système de windows les fichiers suivants : <ul style="list-style-type: none"> <li>- klgcptini.dat - fichier non malicieux</li> <li>- ps.a3d - un fichier log contenant des informations sur le compte mail</li> <li>- qm.dll - copie de sndu32.dll</li> <li>- qm.sys - copy de sndu32.sys</li> <li>- sndu32.dll,sndu64.sys - détectée par les antivirus comme l'alias du troyen</li> </ul> </li> <li>- Il se connecte à des sites suspects et tente de télécharger et charger des fichiers malveillants</li> <li>- Le troyen s'inscrit dans la base de registre pour pouvoir s'exécuter automatiquement au démarrage de windows</li> <li>- Le troyen ajoute les clés suivantes : <pre> HKEY_CURRENT_USER\Software\RIT\The Bat! HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Enum\Root\LEGACY_SNDU64\0000 Service = "sndu64" Legacy = "dword:00000001" ConfigFlags = "dword:00000000" Class = "LegacyDriver" ClassGUID = "{8ECC055D-047F-11D1-A537-0000F8753ED1}" DeviceDesc = "SoundDriver SDB64"  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Control\SafeBoot\Minimal\sndu32.sys default = "Driver"  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Control\SafeBoot\Minimal\sndu64.sys default = "Driver" </pre> </li> <li>- Si la machine victime tourne sur Windows 98 ou ME, le troyen crée les clés suivantes : <pre> HKEY_LOCAL_MACHINE\System\CurrentControlSet\ Control\MPRServices\TestService DllName = "sndu32.dll" EntryPoint = " MMXChckIDT " StackSize = "dword:00000000" secureUID = "{random UID}" </pre> </li> <li>- pour bloquer le fonctionnement du firewall windows, il crée les clés suivantes : <pre> HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\ Services\SharedAccess\Parameters\FirewallPolicy\ StandardProfile\AuthorizedApplications\List %Windows%\Explorer.EXE = </pre> </li> </ul> |

|   |  |
|---|--|
|   | <p>"%Windows%\Explorer.EXE.*:Enabled:explorer"</p> <p>- il supprime également l'entrée suivante de la base de registre pour désactiver l'option "set Internet Connection Sharing" et le firewall Windows :</p> <p>HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess<br/>Start = "dword:00000003"</p>   |
| <b>Degré d'infection à l'échelle Internationale</b> | moyennement élevé (Niveau 3)   |
| <b>Degré d'infection à l'échelle nationale</b>      | Limité   |
| <b>Propagation</b>                                  | Propagation via mail   |
| <b>Pour plus de détails</b>                         | <p><a href="http://uk.trendmicro-europe.com/consumer/vinfo/encyclopedia.php?LYstr=VMAINDATA&amp;vNav=3&amp;VName=BKDR_HAXDOOR.GM">http://uk.trendmicro-europe.com/consumer/vinfo/encyclopedia.php?LYstr=VMAINDATA&amp;vNav=3&amp;VName=BKDR_HAXDOOR.GM</a></p> <p>- <a href="http://www.sophos.fr/virusinfo/analyses/trojhxdoorin.html">http://www.sophos.fr/virusinfo/analyses/trojhxdoorin.html</a></p> <p>- <a href="http://www.symantec.com/avcenter/venc/data/backdoor.haxdoor.j.html">http://www.symantec.com/avcenter/venc/data/backdoor.haxdoor.j.html</a></p> |

## MESURES PREVENTIVES

Si vous pensez avoir été infecté, il faudra :

- Désactiver la restauration automatique du système (Windows Me/XP).
- Au cas où vous avez un anti-virus :

Redémarrer en mode de récupération en utilisant le CD d'installation Windows  
Mettre à jour la base de signature de votre antivirus ainsi que sa base de définition de virus.  
Scanner le système.  
Supprimer les fichiers malveillants  
Supprimer toutes les clés ajoutées dans la base de registre.  
Restaurer les clés supprimer à partir du backup

- Au cas où vous en avez pas installé un antivirus et si vous êtes un utilisateur domestique, vous pouvez installer gratuitement l'un des anti-virus proposés par l'Agence [http://www.ansi.tn/fr/outils\\_domestique.htm](http://www.ansi.tn/fr/outils_domestique.htm)

Il est toujours conseillé de prendre les mesures préventives suivantes :

- Ne pas ouvrir des fichiers joints de messages aux quels vous ne vous attendez pas.
- Éviter de télécharger des et d'installer des applications d'origines suspectes
- Isoler immédiatement les machines infectées pour empêcher une plus ample propagation au sein de votre réseau.
- Configurer votre serveur mail de sorte à bloquer ou de supprimer tout email ayant des fichiers joints communément utilisés pour la propagation de virus
- Utiliser des firewalls personnels vous permettant de surveiller les connexions en entrées et en sortie de votre système.

**Source: Cert-TCC**  
**Agence Nationale de la Sécurité Informatique**