

**Objet** : Apparition d'un cheval de Troie baptisé "**Ginwui**" ou "**BackDoor-CKB!cfaae1e6**" qui exploite la vulnérabilité de l'éditeur de texte Microsoft Word . Le troyen se propage à travers un e-mail avec un fichier MS-Word, portant le nom **CSRSE.EXE**, en attachement.

**Systèmes concernés** :Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP

<b>Effets</b>	<p>Lorsque le cheval de Troie s'exécute, il tente de :</p> <ul style="list-style-type: none"> <li>- Créer, supprimer, rechercher lire et écrire des fichiers et des dossiers</li> <li>- S'inscrire dans la base de registre afin de pouvoir s'exécuter automatiquement au démarrage de Windows.</li> <li>- S'accrocher à des APIs pour se camoufler</li> <li>- Ouvrir une porte dérobée et reste en écoute des connections provenant de l'attaquant pour recevoir des instructions</li> <li>- Collecter des informations sur le système affecté</li> <li>- Accéder au shell cmd.exe</li> <li>- Prendre des captures d'écran et les sauvegarder dans le dossier d'installation de Windows sous le nom <b>Capture.bmp</b></li> <li>- Verrouiller, redémarrer et arrêter Windows</li> <li>- Manipuler des services, démarrer et arrêter des processus</li> </ul>
<b>Signes visibles d'infection</b>	<ul style="list-style-type: none"> <li>- Le cheval de Troie essaie de se connecter au site web suivant: <a href="http://localhosts.3322.org">http://localhosts.3322.org</a></li> <li>- Il tente d'ajouter les fichiers suivants dans le répertoire système: <b>Winguis.dll, IsPubDRV.sys, RVdPort.sys , DetPort.sys</b></li> <li>-Il tente d'ajouter la clé suivante dans la base de registre: HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows "Applnit_DLLs" = "%System%\Winguis.dll"</li> </ul>
<b>Degré d'infection à l'échelle Internationale</b>	Limité (Niveau 2)
<b>Degré d'infection à l'échelle nationale</b>	Limité
<b>Propagation</b>	via courrier électronique
<b>Pour plus de détails</b>	<p><a href="http://www.f-secure.com/v-descs/ginwui_a.shtml">http://www.f-secure.com/v-descs/ginwui_a.shtml</a>  <a href="http://www.symantec.com/avcenter/venc/data/backdoor.ginwui.html">http://www.symantec.com/avcenter/venc/data/backdoor.ginwui.html</a>  <a href="http://fr.trendmicro-europe.com/enterprise/vinfo/encyclopedia.php?VName=BKDR_GINWUI.A">http://fr.trendmicro-europe.com/enterprise/vinfo/encyclopedia.php?VName=BKDR_GINWUI.A</a></p>

## Solution

### Mesures préventives

- Ne pas ouvrir de messages joints d'un fichier nommé **CSRSE.EXE**.

### Désinfection

Si vous pensez avoir été infecté, il faudra ainsi :

- **Désactiver l'option Restauration du système (Windows Me/XP).**
- **Au cas où vous avez un anti-virus :**
  - **Mettre à jour la base de signature de votre antivirus.**
  - **Effectuer un scan complet du système et supprimer tous les fichiers infectés.**
  - **Supprimer toutes les valeurs ajoutées au registre.**
- **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.**

Source: Cert-TCC  
Computer Emergency Response Team - Tunisian Coordination Center  
Agence Nationale de la Sécurité Informatique