

Objet : Propagation d'une nouvelle variante du ver informatique de mass-mailing baptisée W32.**Mytob.PO@mm** qui peut ouvrir une porte dérobée et tente de désactiver les dispositifs de sécurité sur l'ordinateur affecté.

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

Effets	<p>Une fois activé, le ver Mytob.PO@mm exécute les actions suivantes :</p> <ul style="list-style-type: none">- créer le fichier winsys32.exe sous le répertoire système. - recueillir les adresses email à partir de fichiers ayant une des extensions suivantes : <ul style="list-style-type: none">- .txt- .html- .shtml- .jspx- .cgil- .xmls- .phpq- .aspd- .dbxn- .tbbg- .adbh- .html- .wab <p>- ouvre une porte dérobée en se connectant au serveur o.thinki.co.uk via le port TCP 8585 pour rester à l'écoute d'instructions à distance notamment pour :</p> <ul style="list-style-type: none">* Effectuer des commandes IRC,* Envoyer des emails,* Télécharger des fichiers,* Retrouver des informations confidentielle sur la machine infectée.
Signes visibles d'infection	<p>- Le ver Mytob.PO@mm s'envoie comme un attachement d'e-mail aux adresses e-mail rassemblées et ce en utilisant son propre moteur de SMTP.</p> <p>Expéditeur : L'adresse source utilisée par le ver comprend un nom de domaine aléatoire précédé de :</p> <p>spm@ fcnz@ www@ secur@ abuse@</p> <p>- Le ver peut aussi utiliser comme adresse d'envoi de l'email une adresse trouvée sur la machine infectée.</p> <p>Sujet : Le sujet du message envoyé est soit "Account Alert" soit constitué d'une chaîne de caractères aléatoire</p> <p>Message : Dear Valued Member, According to our terms of services, you will have to confirm your e-mail by the following link, or your account will be suspended within 24 hours for security reasons. http://www.[DOMAIN]/confirm.php?account=[E-MAIL] After following the instructions in the sheet, your account will not be interrupted and will continue as normal. Thanks for your attention to this request. We apologize for any inconvenience.</p>

	Sincerely, [RANDOM_NAME] Abuse Department <u>Nota</u> : L'URL incluse dans l'email contient un lien vers une copie du ver à l'adresse : [http://]194.85.25.16/mysqladmin/Confirmatio[REMOVED]
Degré d'infection à l'échelle Internationale	Limité (Niveau 2)
Degré d'infection à l'échelle nationale	Limité
Propagation	Propagation via mail
Pour plus de détails	http://www.sarc.com/avcenter/venc/data/w32.mytob.po@mm.html

MESURES PREVENTIVES

Il est conseillé aux administrateurs réseau de définir des ACL bloquants les ports non nécessaires tel que le port 8585.

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 :
 - Mettre à jour la base de signature de votre antivirus ainsi que sa base de définition de virus.
 - Scanner le système et supprimer tous les fichiers infectés.
 - Supprimer toutes les clés ajoutées dans la base de 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 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.
 - 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 e-mail 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
 Computer Emergency Response Team - Tunisian Coordination Center
 Agence Nationale de la Sécurité Informatique
 Ministère des Technologies de la Communication