

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Alerte de virus NEWLOVE

Conditions d'utilisation de ce document : <http://www.certa.ssi.gouv.fr/certa/apropos.html>
Dernière version de ce document : <http://www.certa.ssi.gouv.fr/site/CERTA-2000-ALE-002>

1 Résumé

Un nouveau virus appelé "NewLove" mutant de "ILOVEYO" est en train de se propager sur le réseau. Comme ce dernier il est écrit en VBScript et se propage par e-mail, dont l'objet commence par "FW" et comportant une pièce jointe portant l'extension .vbs. Cette pièce jointe porte un nom aléatoire à chaque envoi.

Si l'utilisateur double-clique sur la pièce-jointe, le ver va s'exécuter à l'aide de WSH.

2 Origine

- Nous ne disposons pas encore des sources du ver.
- Informations obtenues sur les groupes de news.
- Informations données par un de nos partenaire.
- Lu sur les sites de NAI (Macfee) et Symantec (Norton).

3 Risque

- Le risque est élevé si les utilisateurs ne sont pas sensibilisés.
- Ecrasement des fichiers non utilisés.
- Mode de propagation par messagerie.
- Le virus nécessite une mémoire importante ce qui ralentie sa propagation.

4 Principe

4.1 Propagation

Quand le ver est lancé, il se **recopie dans le dossier Windows** en prenant un nom de l'un des documents récemment ouvert, avec une extension prise alatoirement dans la liste : Doc, Xls, Mdb, Bmp, Mp3, Txt, Jpg, Gif, Mov, Url, Htm, Txt et en y ajoutant l'extension .vbs.

Il s'auto-modifie en ajoutant des commentaires alatoires à son code après chaque infection afin de troubler sa détection.

Ensuite, le programme cherche à se propager en exploitant le carnet d'adresses d'Outlook de la victime (de la même façon qu'ILOVEYOU).

4.2 Systèmes impactés

Comme pour ILOVEYOU tous les systèmes Windows sont concernés.

5 Fichiers infectés

1. Il modifie les entrées suivantes dans la base de registres:

- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\
- HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices\

2. NEWLOVE s'attaque à **tous les fichiers** qui ne sont pas en cours d'utilisation, en les remplaçant par lui même.

6 Solution

1. Mise en oeuvre des recommandations (CERTA-2000-REC-001 du 15 mai 2000), faites à la suite de ILOVEYOU et en particulier d'interdire l'exécution des scripts .vbs.
2. Mis à jour des anti virus.
3. Application des règles élémentaires de précaution :

- (a) **NE JAMAIS CLIQUER IMMEDIATEMENT sur une pièce-jointe.**
- (b) **NE JAMAIS MASQUER LES EXTENSIONS dans l'explorateur de Windows.**