Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

S . G . D . S . N
Agence nationale de la sécurité des systèmes d'information
CERTA

Paris, le 29 janvier 2002
N° CERTA-2002-ALE-003

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Propagation importante du virus « W32.Myparty@mm »

Gestion du document

Référence	CERTA-2002-ALE-003
Titre	Propagation importante du virus « W32.Myparty@mm »
Date de la première version	29 janvier 2002
Date de la dernière version	–
Source(s)	Sophos
Pièce(s) jointe(s)	Aucune

TAB. 1 – *gestion du document*

Une gestion de version détaillée se trouve à la fin de ce document.

1 Risque

– Compromission du système ;
– propagation d'un ver.

2 Systèmes affectés

Toutes les plateformes Windows 9x et plateformes Windows 32 bits.

3 Résumé

Le ver Win32 ayant pour nom « W32.Myparty@mm » ou encore « W32/Myparty@mm » se propage actuellement à grande vitesse par un mél dont sujet est « `new photo from my party!` ».

4 Description

Le mél envoyé a comme pièce jointe l'un des deux fichiers suivants :

- `www.myparty.yahoo.com`;
- `www.photos.yahoo.com`.

Certaines personnes ont été trompées en pensant que la pièce jointe était un lien vers un site web.

Quand la pièce jointe est exécutée, le ver envoie une copie de lui-même à toutes les entrées du carnet d'adresses de Windows en utilisant un moteur SMTP intégré et place une copie du fichier dans `c:` sur windows NT/2K, XP, ou sur le répertoire `Recycled` sur windows 9x/ ME, dans un fichier ayant pour nom `regctrl.exe`.

Pour les versions US le ver place également une copie du cheval de troie `Troj/Msstake-A` dans le répertoire de démarrage de l'utilisateur. Le cheval de troie est présent dans un fichier nommé `msstask.exe` qui permet l'ouverture d'une porte dérobée sur la machine compromise.

De plus, le ver envoie un mél à l'adresse `napster@gala.net` et lance le navigateur sur le site WEB suivant : `http://www.disney.com`.

5 Solution de prévention

Suivre les recommandations de la note CERTA-2000-INF-002 concernant les pièces jointes :

- mettre à jour son antivirus ;
- ne pas exécuter les pièces jointes sans vérification de leur bien-fondé. En particulier le fait de recevoir une pièce jointe d'une personne connue n'est pas une garantie de l'inocuité de l'attachement.

6 Solution

Après avoir déconnecté la machine infectée du réseau, mettez à jour votre antivirus et vérifiez votre système,

vous pouvez également vérifier qu'il n'existe pas de processus `msstask.exe` dans la barre des tâches, dans le cas contraire il est nécessaire d'arrêter ce processus et d'enlever le fichier `msstask.exe` qui se trouve dans votre répertoire de démarrage (il est nécessaire de redémarrer la machine en mode DOS pour supprimer ce fichier).

7 Documentation

- Avis de Fsecure :
  http://www.europe.f-secure.com/v-descs/myparty.shtml
- Encyclopédie des virus de Symantec :
  http://www.symantec.com/avcenter/venc/data/w32.myparty@mm.html
- Bulletin de sécurité de Sophos :
  http://www.sophos.com/virusinfo/analyses/w32mypartya.html

Gestion détaillée du document

29 janvier 2002 version initiale.