Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 26 juillet 2001
N° CERTA-2001-ALE-009-001

Affaire suivie par :
CERTA

BULLETIN D'ALERTE DU CERTA

Objet : Propagation importante du virus SirCam

Gestion du document

Référence	CERTA-2001-ALE-009-001
Titre	Propagation importante du virus SirCam
Date de la première version	26 juillet 2001
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

- Divulgation de documents et perte de confidentialité ;
- propagation d'un ver.

2 Systèmes affectés

Toutes les plateformes Windows 9x et dans certains cas les autres plateformes Windows 32 bits.

3 Résumé

Des remontées d'informations, nous apprennent que le ver SirCam se propage à très grande vitesse sur les réseaux français.

4 Description

Le virus SirCam-A aussi appelé W32/SirCam@mm, Backdoor.Sircam ou encore W32.Sircam.Worm@mm est un ver utilisant pour se propager les pièces jointes dans un mél ainsi que les fichiers partagés et non protégés sous Windows.

Il se présente actuellement sous la forme d'un mél écrit en anglais ou espagnol invitant l'utilisateur à exécuter une pièce jointe à ce courrier.

Les pièces jointes sont des fichiers de la machine contaminée de l'émetteur du message possèdant une double extension en `.jpg.com`, `.mpg.pif` par exemple, afin de tromper la vigilance des usagers.

Si le fichier attaché est ouvert, le ver installe les fichiers suivants :
`C:\RECYCLED\SirC32.exe` ainsi que `SCam32.exe` dans le repertoire `Windows\System`.
Plusieurs clés de la base des registres sont aussi créées ou modifiées :

```
HKCR\exefile\shell\open\command\Default="C:\recycled\SirC32.exe" "%1" %*
HKLM\Software\Microsoft\Windows\CurrentVersion\ RunServices\Driver32=C:\WINDOWS\SYSTEM\SCam32.exe
HKLM\Software\Sircam
```

En plus de s'installer, et de se propager sous cette forme, le virus peut avoir d'autres effets :

- diffusion par mél de fichiers trouvés sur le disque dur de la machine contaminée puis infectés ;
- suppression aléatoire de fichiers du disque dur voire effacement complet ;
- remplissage de l'espace restant sur le disque dur par ajout de texte au fichier `\Recycled\sircam.sys`.

L'effet nuisible principal de ce virus, est certainement la diffusion non contrôlée de documents.

Ce ver a la particularité de possèder son propre service SMTP de façon à envoyer ses messages aux correspondants du carnet d'adresses Outlook ainsi qu'aux adresses trouvées dans les fichiers temporaires d'Internet Explorer.

Il recherche aussi les répertoires partagés sans protection sur le réseau.

Lorsqu'il en trouve, il tente de s'installer dans le répertoire `Recycled` sous le nom `SirC32.exe` et de renommer `rundll32.exe` en `run32.exe` pour s'y substituer dans le répertoire Windows du disque partagé s'il existe.

En cas de succès, le fichier `autoexec.bat` est modifié de façon à exécuter `Rundll32.exe` au démarrage.

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.

Suivre les recommandations de l'avis CERTA-2001-ALE-002 concernant les partages de fichiers :

- Bloquer les ports concernant Netbios sur le garde-barrière : 135, 137, 138, 139 TCP et UDP ;
- mettre à niveau les règles de sécurité sur les fichiers et principalement les ressources partagées :
  - supprimer les partages non authentifiés ;
  - mettre des mots de passe sur tout partage Windows 9x ;
  - renforcer les mots de passe existants ;
  - renforcer les permissions sur les partages de Windows NT/2000.

6 Solution en cas de contamination

Après avoir déconnecté la machine infectée du réseau, mis à jour votre antivirus et vérifié que votre système affiche tous les fichiers et ne masque aucune extension suivez ces instructions dans l'ordre :

1. Supprimer tous les fichiers `\windows\SIrC32.exe` et `Scam32.exe` s'ils existent ;
2. Si`run32.exe` existe, alors supprimer `rundll32.exe` et renommer `run32.exe` en `rundll32.exe` ;

3. modifier les clés de la base des registres comme suit :
   - supprimer les clés
     `\HKEY_LOCAL_MACHINE\Software\Sircam;`
     `\HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesirCam;`
   - et changer la valeur de la clé (*Ne surtout pas supprimer cette clé !*)
     `\HKEY_CLASSES_ROOT\exefile\shell\open\command`
     en y remettant la valeur `"%1" %*`.
4. Supprimer, si elle existe, la ligne
   `@Win \recycled\sirc32.exe`
   du fichier autoexec.bat ;
5. supprimer le fichier `Sircam.sys` s'il existe ;
6. parcourir tout le système avec l'antivirus et supprimer tous les fichiers détectés par ce dernier.

7 Solution

Mettre à jour les bases de signatures des logiciels anti-virus.

8 Documentation

- Avis de Fsecure :
  http://www.europe.f-secure.com/v-descs/sircam.shtml
- Encyclopédie des virus de Symantec :
  http://www.symantec.com/avcenter/venc/data/w32.sircam.worm@mm.html
- Bulletin de sécurité de Sophos :
  http://www.sophos.com/virusinfo/analyses/w32sircama.html

Gestion détaillée du document

24 juillet 2001 version initiale.

26 juillet 2001 seconde version : dans les solutions, la supression de la clé
`HKCR\exefile\shell\open\command\Default="C:\recycled\SirC32.exe" "%1" %*`
engendre un disfonctionnement des systèmes traités.