



Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PREMIER MINISTRE

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

Paris, le 31 août 2000
N° CERTA-2000-AVI-041

Affaire suivie par :
CERTA

AVIS DU CERTA

Objet : Ver sous Windows : W32/Apology

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-AVI-041>

Gestion du document

| | |
|-----------------------------|--------------------------------|
| Référence | CERTA-2000-AVI-041 |
| Titre | Ver sous Windows : W32/Apology |
| Date de la première version | 31 août 2000 |
| 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

- Exécution de commandes ;
- Propagation de virus.

2 Systèmes affectés

- Microsoft Windows 9x ;
- Microsoft Windows 2000 ;
- Microsoft Windows NT.

3 Description

Le ver Apology remplace le fichier wsock32.dll par une version modifiée dans le but de surveiller le trafic réseau. Lorsque l'utilisateur d'une machine infecté expédie un mël, un second est automatiquement transmis au même destinataire.

Ce second message ne contient ni sujet, ni corps mais un fichier exécutable en pièce jointe qui, une fois exécuté, installe le ver sur la machine du destinataire. Ce fichier joint est susceptible de porter l'un des noms suivants :

- README.TXT.pif

- I_wanna_see_YOU.TXT.pif
- MATRiX_Screen_Saver.SCR
- LOVE_LETTER_FOR_YOU.TXT.pif
- NEW_playboy_Screen_saver.SCR
- BILL_GATES_PIECE.JPG.pif
- TIAZINHA.JPG.pif
- FEITICEIRA_NUA.JPG.pif
- Geocities_Free_sites.TXT.pif
- NEW_NAPSTER_site.TXT.pif
- METALLICA_SONG.MP3.pif
- ANTI_CIH.EXE
- INTERNET_SECURITY_FORUM.DOC.pif
- ALANIS_Screen_Saver.SCR
- READER_DIGEST_LETTER.TXT.pif
- WIN_\$100_NOW.DOC.pif
- IS_LINUX_GOOD_ENOUGH!.TXT.pif
- QI_TEST.EXE
- AVP_Updates.EXE
- SEICHO-NO-IE.EXE
- YOU_are_FAT!.TXT.pif
- FREE_xxx_sites.TXT.pif
- I_am_sorry.DOC.pif
- Me_nude.AVI.pif
- Sorry_a_bout_yesterday.DOC.pif
- Protect_your_credit.HTML.pif
- JIMI_HMNDRIX.MP3.pif
- HANSON.SCR
- F*****_WITH_DOGS.SCR
- MATRiX_2_is_OUT.SCR
- zipped_files.EXE
- BLINK_182.MP3.pif

Apology bloque l'accès aux sites internet de différents éditeurs d'anti-virus et empêche d'envoyer des mails à ces éditeurs. Il tente également de se connecter sur un site dans le but de récupérer des composants à exécuter sur la machine infectée.

Apology crée les fichiers suivants dans le répertoire d'installation de Windows :

- IE_PACK.EXE
- MTX_.EXE
- WIN32.DLL
- WSOCK32.MTX

Le fichier WININIT.INI est modifié afin de lancer WSOCK32.MTX à la place de WSOCK32.DLL lors du redémarrage de la machine.

Deux entrées sont également ajoutées à la base de registre :

- HKLM\Software\[MATRix]
- HKLM\Software\Microsoft\Windows\CurrentVersion\Run
SystemBackup = "C:\WINDOWS\MTX_.EXE"

Le fichier MTX_.EXE tente toute les deux minutes d'établir une connexion TCP sur le port 1137.

4 Solution

- Bloquer le port 1137 afin de stopper la connexion TCP ;
- Mettre à jour votre anti-virus.

5 Documentation

Document Sophos :
<http://www.sophos.com/virusinfo/analyses/w32apology.html>

Gestion détaillée du document

31 août 2000 version initiale.