W32/Petik-K

Alias: Troj/Petik-K

Type: Ver Win32

Sujet : " Loft Story News...

Corps du texte : " The last video of the program "

Pièce jointe : loft_story.exe

Description:
W32/Petik-K est un ver de messagerie qui prétend se connecter sur le site web du célèbre programme TV français "Loft Story" pour essayer de se propager.

Le virus se copie dans le répertoire Windows sous le nom loft_story.exe et dans le répertoire System de Windows sous le nom loft.exe. Il change le fichier WIN.INI pour que loft.exe soit automatiquement exécuté toute les fois que Windows est démarré. Il affiche ensuite une boîte de dialogue titrée " Loft Story " et le corps de texte " I'm fucking the Loft Story " avant de quitter.

Lorsqu'il est exécuté à partir du répertoire System de Windows, le virus crée la clé de registre HKCU\Software\Microsoft\PetiK. Il place le fichier loft.htm (que Sophos Anti-Virus détecte comme Troj/Petik-K) dans le sous-répertoire Startup de Windows et attend une connexion Internet.

Sujet : " Loft Story News...
Corps du texte : " The last video of the program "
Pièce jointe : loft_story.exe"

Le 28 de chaque mois, le virus configurera les clés de registre.

HKCU\Software\Microsoft\Internet Explorer
\Main\Start Page = "http://www.loftstory.fr"

HKLM\Software\Microsoft\Windows\CurrentVersion
\RegisteredOrganization= "LoftStory"

HKLM\Software\Microsoft\Windows\CurrentVersion
\RegisteredOwner = "Aziz, Kenza, Loanna, etc..."

Il affiche alors le message " New Worm Internet coded by PetiK (c)2001 ".

Le fichier HTML placé par W32/Petik-K est détecté par Sophos Anti-Virus comme Troj/Petik-K et contient un VBScript qui modifie les clés de registre suivantes :

HKLM\Software\Microsoft\Windows\CurrentVersion
\Run\ActiveX 1.0 = "C: \ActiveX.vbs"

HKCU\Software\Microsoft
\Internet Explorer\Download Directory = "C:\".

Il changera aussi l'entrée de registre pour la page d'accueil d'Internet Explorer, configurée pour télécharger le fichier VBScript à partir de http://www.ctw.net.

<< Retour Page Virus **<< Retour Page Webmaster**

- Dernière mise à jour du site le : 1 Octobre 2001 à 11:45:43 -