PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 524 di martedì 26 marzo 2002

Attenzione: worm in agguato

Segnalato un falso screen saver che tenta di cancellare i file presenti sull'hard disk.

Le aziende produttrici di antivirus hanno innalzato il livello di attenzione per la diffusione di una variante del worm MyLife, che si propaga come allegato di un messaggio di posta elettronica.
Attualmente il virus e' stato rilevato in Asia ed Australia.
L'e-mail invita il mittente a cliccare sul file "cari.scr" allegato, contenente una caricatura dell'ex-presidente USA Bill Clinton.

Se l'utente cede alla tentazione ed apre il file, appare una vignetta immagine e il virus si autoinvia attraverso Outlook a tutti gli indirizzi contenuti nell'address book e utilizzando i servizi di MSN.

Il messaggio ha le seguenti caratteristiche:
Da: nome-dell'utente-infetto
A: nome-casuale-all'interno-dell'address book
Oggetto: bill caricature
Testo: Hiiiii
How are youuuuuuuu?
look to bill caricature it's vvvery verrrry
ffffunny :-) :-)
i promise you will love it? ok
buy
========No Viruse Found========
MCAFEE.COM

Allegato: CARI.SCR

Il worm copia se stesso nella directory c:windowssystem come CARI.SCR e aggiunge al registro di configurazione del sistema la seguente chiave:
[HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun]
"win" = "%SysDir%cari.scr"

Si tratta di un worm potenzialmente distruttivo in quanto, dopo essersi inviato, tenta di cancellare i file con le seguenti estensioni: *.sys (directory Windows), *.vxd, *.sys, *.ocx, *.nls (directory Windows System)

Il worm inoltre tenta di eliminare tutti i file nelle posizioni: c:, d:, e:, f: per rendere il sistema inutilizzabile.