PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 3 - numero 450 di martedì 27 novembre 2001

Allarme virus!

Nuove segnalazioni di due "vecchi" virus che si diffondono via e-mail. Come individuarli.

La diffusione di una variante del virus BadTrans e del virus Aliz, individuato per la prima volta a maggio, e' stata segnalata dalle maggiori aziende di antivirus.
Entrambi i virus "colpiscono" via e-mail.

Il virus Aliz (Win32.Aliz, W95/Aliz.a), scritto in linguaggio Assembly e lungo solo 4 Kb, e' in grado di auto-inviarsi a tutti gli indirizzi contenuti nella rubrica di Windows tramite il server SMTP di default.

Il soggetto del messaggio infetto e' composto dalla combinazione di alcune parole prese a caso da una lista, non varia invece "Whatever.exe", il nome dell'allegato che contiene il codice del virus.

Il corpo della e-mail e' un messaggio MIME multi-parte in HTML che, sfruttando una vulnerabilita' dei sistemi sui quali sono installati Outlook e Internet Explorer 5.0 e 5.01 e su cui non sia stata applicata un'apposita patch di Microsoft, e' in grado di eseguire il proprio allegato durante la lettura del messaggio, senza ulteriori interventi dell'utente.

Il secondo virus segnalato e' invece una variante del worm BadTrans (BadTrans.B), che sfrutta la stessa vulnerabilita' della quale si serve Aliz.
Questo worm invia una serie di messaggi di posta elettronica senza testo e con allegati che hanno doppia estensione.

Il file allegato ha un nome presente nella lista seguente:
FUN, HUMOR, DOCS, S3MSONG, Sorry_about_yesterday, ME_NUDE, CARD, SETUP, SEARCHURL, YOU_ARE_FAT!, HAMSTER, NEWS_DOC, New_Napster_Site, README, IMAGES, PICS.
La prima estensione dell'allegato e' uno dei valori: DOC, MP3, ZIP; mentre la seconda e': pif, scr.

Il worm installa sui sistemi infettati il file KDLL.DLL che contiene un programmino il cui scopo e' impossessarsi delle password dell'utente.

---

www.puntosicuro.it