PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 674 di venerdì 29 novembre 2002

Computer a rischio

Segnalata la diffusione di un nuovo worm distruttivo. Conosciamone le caratteristiche.

Ha già creato danni in alcuni Paesi europei il worm Winevar, rilevato per la prima volta in Corea, contenuto in un file eseguibile allegato ad una e-mail.

Per non essere infettati da Winevar (detto anche HLLM.Seoul, Korvar, I-Worm.Winevar, Braid.C) non è sufficiente avere l'accortezza di non aprire allegati sospetti. E' necessario che sia l'antivirus sia il sistema siano aggiornati.
Il worm infatti è cerca di eseguirsi automaticamente da una mail infetta utilizzando una nota vulnerabilità di Microsoft Internet Explorer. Inoltre Winevar utilizza una falla del componente Microsoft VM ActiveX .

Il worm è contenuto nell'allegato di una email che può avere caratteristiche variabili. Eccone un esempio:
Soggetto: Re: AVAR(Association of Anti-Virus Asia Reseachers)
Testo: AVAR(Association of Anti-Virus Asia Reseachers) - Report.
Invariably, Anti-Virus Program is very foolish.
Attachment:
WINxxx.TXT (12.6 KB) MUSIC_1.HTM
WINxxx.GIF (120 bytes) MUSIC_2.CE
Le sequenze di caratteri "xxx" stanno ad indicare lettere casuali.

Secondo quanto riportato da Symbolic, quando il file viene eseguito, il worm copia se stesso nella directory System di Windows come WINxxxx.PIF, dove xxxx sono caratteri casuali, modifica la configurazione del sistema in modo da eseguirsi ad ogni riavvio.

Il worm Winevar, quando attivo in memoria, cerca continuamente di terminare alcuni processi e cerca nei dischi locali file e directory relativi agli antivirus per eliminarli.
A causa di un baco in questo processo, in realta' il worm cancella tutti i file presenti sul disco.

Il worm cerca gli indirizzi di posta elettronica a cui inviarsi dai file *.HTM e *.DBX.
