PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 580 di mercoledì 19 giugno 2002

Attenzione agli allegati!

Si diffonde via e-mail un worm tutto italiano. Conosciamone le caratteristiche.

"Qualsiasi cosa fai, falla al meglio".
Pare un saggio consiglio; ma nel caso vi giunga una e-mail con questo soggetto, anche se il mittente è una persona conosciuta, diffidate e non aprite l'allegato in quanto potrebbe contenere un worm.

E' stata infatti segnalata la diffusione di Higuy-A, un worm italiano che si propaga via e-mail e che, per indurre l'utente ad eseguire l'allegato, utilizza un linguaggio semplice, frasi "tipo" utilizzate per accompagnare file allegati.

Il messaggio ha le seguenti caratteristiche:
Soggetto
E' scelto tra i seguenti:
-Qualsiasi cosa fai,falla al meglio.
-Incredible...
-Urgente! (vedi allegato)

Testo
Nella versione italiana inizia sempre con "Ciao" e si conclude con "A presto". Il testo è scelto tra:
-okkio all'allegato ;-)
-apri subito l'allegato,e' molto interessante.
-devi assolutamente vedere il file che ti ho allegato.

Ne esiste anche una versione in inglese:
Hello,
see this interesting file.
Bye.

Allegato
L'allegato infetto puo' essere denominato: TATOO.EXE, EURO.EXE o TETTONA.EXE.

A quanto si è appreso da Symbolic, se l'allegato viene eseguito, viene visualizzato un finto messaggio di errore sul file VBRUN49.DLL ed il worm mette una copia di se stesso nella directory di Windows: il file viene chiamato DLLMGR32.EXE ed e' richiamato ad ogni avvio del sistema mediante la chiave di registro:
HKLMSoftwareMicrosoftWindowsCurrentVersionRunDllManager = dllmgr32.exe
(dove indica la directory del sistema operativo, tipicamente C:WINDOWS o C:WINNT).
Il worm, non distruttivo, ricava poi gli indirizzi di altri utenti dal Windows Address Book per propagare l'infezione via e-mail.