PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 587 di venerdì 28 giugno 2002

Worm: quando l'apparenza inganna...

Un messaggio infetto si puo' mascherare usando come mittente l'indirizzo di una azienda antivirus.

Yaha.E non è il primo caso di worm che, grazie a caratteristiche mutevoli, tenta di ingannare gli utenti sfruttando la popolarità di marchi noti.
Tuttavia questo worm, che falsifica le informazioni relative al vero mittente, ha fatto arrabbiare molti utenti di Sophos che, vedendosi recapitare una e-mail infetta dall'indirizzo della nota azienda di antivirus, hanno richiesto spiegazioni alla società.

Sophos ha assicurato ai suoi utenti che i messaggi infetti non provengono dall'azienda; è il worm che inserisce come mittente delle e-mail infette indirizzi "falsi".

La mail "sospetta" è riconoscibile dal fatto che il subject è una frase in inglese e l'inizio del messaggio può essere uno dei tre seguenti: "Hi Check the Attachment...See u", "Attached one Gift for u...", "WOW CHECK THIS".

Il worm Yaha-E si sta diffondendo anche in un'altra versione, per la quale la mail risulta inviata da "MAILER-DEMON@domain.com" e ha come linea soggetto "Undeliverd Mail Returned to Sender(nome casuale)". Il testo del messaggio, poi, riprende il messaggio tipico di una email che non si è riusciti a spedire correttamente.

Per evitare problemi il consiglio principale è non aprire l'allegato infetto e aggiornare tempestivamente il software antivirus.
