PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 469 di martedì 08 gennaio 2002

Anno nuovo, virus nuovi

Due nuovi worm si sono diffusi nei giorni scorsi via e-mail...

Via e-mail sono stati recapitati nelle scorse settimane milioni di auguri di buone feste.
Ma non tutte le e-mail inviate durante le festivita' sono portatrici di buon augurio e cordialita'...

E' il caso dei messaggi contenenti gli attach infettati da due nuovi virus che da pochi giorni sono comparsi in rete: Scherzo (detto anche Zoher o Sheer) e ZaCker.
"Scherzo" e' un worm della posta elettronica che si diffonde tramite un lungo messaggio in italiano con un allegato denominato javascript.exe.
Il worm sfrutta una la vulnerabilita' di Internet Explorer 5.0 e 5.01 che , sui sistemi nei quali non e' stata installata l'apposita patch, consente l'esecuzione automatica di un attach alla lettura della mail.

Sui sistemi non aggiornati l'attachment e' in grado di eseguirsi automaticamente durante la lettura della mail. Una volta lanciato, il worm si spedisce a tutti gli indirizzi del Windows Address Book, utilizzando il server di posta di default.

Le e-mail inviate da Zoher hanno questo aspetto:
Da: nome dell'utente infetto
A: indirizzo-casuale-preso-dal-WAB
Soggetto: Fw: Scherzo!
Allegato: javascript.exe
Messaggio: [Il messaggio e' molto lungo, ne riportiamo solo l'inizio] Con questa mail ti e stata spedita la FortUna; non la fortuna e basta, e neanche la Fortuna con la F maiuscola, ma addirittura la FortUna con la F e la U maiuscole. Qui non badiamo a spese. Da oggi avrai buona fortuna, ma solo ed esclusivamente se ti liberi di questa mail e la spedisci a tutti quelli che conosci...

"Scherzo" non si installa nel sistema, quindi e' piuttosto semplice da rimuovere anche manualmente.
Gli esperti di F-Secure consigliano "Prima di tutto, se non lo si e' gia' fatto, occorre applicare le patch di sicurezza sopra indicate; riavviare poi il sistema e cancellare i messaggi infetti dalle caselle di posta. L'allegato infetto javascript.exe puo' essere cancellato manualmente o tramite FSAV.".

Il virus ZaCker (W32.Maldal.D@mm), segnalato nei giorni scorsi, e' invece molto piu' pericoloso e distruttivo.
Anche Zacker si diffonde via e-mail ed e' contenuto in un messaggio il cui oggetto contiene la parola "ZaCker", e con allegato un file ".exe" di 27 KB.
Se l'allegato viene aperto, il virus si autoinvia a tutti gli indirizzi presenti nella rubrica del programma di posta elettronica e cerca di distruggere molti file memorizzati sul computer.
