PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 6 - numero 1144 di giovedì 16 dicembre 2004

Attenzione alle finte cartoline di auguri

Si diffonde rapidamente, tramite un e-mail di "Buon Natale", un insidioso worm. Come riconoscerlo.

Pubblicità

Sta avendo una rapida diffusione anche in Italia il worm Zafi.D, che si propaga via e-mail camuffandosi in un breve messaggio di Buon Natale, allegato al quale viene inviata la "cartolina" infetta.

La diffusione è favorita anche dal fatto che vi è una versione italiana dell'e-mail, che ha le seguenti caratteristiche:
Da: [nome reperito in un computer colpito dal worm]
Oggetto: Buon Natale!
Messaggio:
Buon Natale!
:) [nome del mittente]
All'interno del messaggio è inoltre presente una piccola immagine di dubbio gusto (attachement di tipo GIF).

Il nome dell'allegato del worm è variabile ed così generato: la parola "postcard" nella lingua dell'utente, alcuni numeri random e una delle estensioni pif, .cmd, .bat, .com or .zip.
Quando il worm viene eseguito, aprendo l'attachment, potrebbe mostrare un falso messaggio di errore: "Error in packed file!"

Il worm modifica alcune impostazioni di sistema e, prima di propagarsi, esegue una scansione del disco rigido cercando di collezionare indirizzi e-mail.
Riguardo alle modalità di diffusione, gli esperti di Symbolic, azienda del settore antivirus, riferiscono che il worm utilizza il proprio motore SMTP per inviare i messaggi infetti. Il worm seleziona la lingua nella quale inviare il messaggio controllando il dominio della e-mail.
Il worm è particolarmente insidioso, Zafi.D cerca di inibire il controllo di firewall e antivirus e al suo interno contiene una backdoor, che ascolta sulla porta 8181, che può essere utilizzata dall'autore del worm per caricare ed eseguire file nel sistema infetto.

---

www.puntosicuro.it