PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 6 - numero 1025 di martedì 15 giugno 2004

Worm multilingue

Si propaga anche con una e-mail in italiano una nuova variante del worm Zafi.

Potrebbe trarre in inganno gli utenti italiani, appassionati di cartoline virtuali, una nuova variante del worm Zafi che si sta diffondendo tramite l'allegato di un messaggio di posta elettronica.
Mentre una prima variante utilizzava una e-mail in lingua ungherese, Zafi.B è multilingue, si serve infatti di messaggi in inglese, italiano, russo, svedese.
Secondo quanto riportato da Symbolic, il worm è presente in un eseguibile compresso nel formato FSG! di dimensione 12800 byte (una volta decompresso il worm risulta di circa 30 KiB), allegato al messaggio.
Nella versione del messaggio in lingua italiana, l'utente è invitato a cliccare su una "cartolina virtuale" allegata nella quale si nasconde in realtà il worm.
Questo il testo del messaggio:
From: Francesca
Oggetto: eTi e stata inviata una Cartolina Virtuale!
Attachment: "link.cartoline.it.viewcard.index.4g345a.pif"
"Ciao! ha visitato il nostro sito, cartolina.it e ha creato una cartolina virtuale per te! Per vederla devi fare click sul link sottostante: http://cartolina.it/asp.viewcard=index4g345a. Attenzione, la cartolina sarà visibile sui nostri server per 2 giorni e poi verrà rimossa automaticamente".

Quando è eseguito, Zafi.B copia se stesso in una cartella di sistema di Windows con un nome casuale e una estensione .DLL e .EXE. "Vari altri file sono creati nella cartella di sistema con un nome casuale e estensione .DLL. .- spiegano gli esperti di Symbolic.
Il worm usa questi file per memorizzare i propri dati. Zafi.B cerca in tutte le cartelle del sistema e copia se stesso come 'winamp 7.0 full_install.exe' o 'Total Commander 7.0 full_install.exe' in quelle che contengono 'share' o 'upload' nel proprio nome.
Zafi.B cerca all'interno della rubrica di Windows e di altri file per cercare di raccogliere degli indirizzi email. Il worm utilizza il proprio motore SMTP per inviare i messaggi infetti. [...]
Zafi.B ferma tutte le applicazioni che hanno 'firewall' o 'virus' all'interno del proprio nome. Vari tool di Windows fra i quali Task Manager e l'Editor di Registro sono disabilitati quando il worm è attivo."

---

www.puntosicuro.it