PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 5 - numero 806 di venerdì 27 giugno 2003

Inganno a...puntate

Alzata la soglia di attenzione per la diffusione di una nuova variante del worm Sobig, che colpisce i sistemi Windows.

La prima versione del worm Sobig ha invaso la rete a maggio; la virulenza sembrava mitigata dal fatto che Sobig avesse una data di scadenza ma, come molti temevano, alla data di scadenza è arrivata puntuale una nuova variante del worm...
La variante B bloccava la propria diffusione il 31 maggio, mentre la variante C (rilevata per la prima volta nello stesso giorno) si disattivava l'8 giugno. A queste ha fatto seguito Sobig.D, uscita il 18 giugno ma con poco successo.

La variante E, rilevata nei giorni scorsi, sembra invece avere un maggiore potenziale infettivo.
Come riportato dagli esperti di Symbolic, "le sue funzionalità non si discostano molto dalle versioni precedenti: il worm si propaga via e-mail tramite un allegato in formato ZIP che contiene a sua volta un file PIF. Se si esegue questo file, il worm infetta il computer, cerca di propagarsi tramite la rete locale e di rispedirsi via e-mail.".
Sobig.E ha un ciclo di vita limitato, come le varianti precedenti. La sua diffusione si arresta il 14 Luglio 2003.

Il messaggio infetto viene creato dal worm con soggetti differenti e casuali (ad esempio Re: Application o Re: Movie), un testo sempre uguale ("Please see the attached zip file for details.") e nomi di file diversi come allegati (ad esempio "your_details.zip").
Il file del worm, DETAILS.PIF, è contenuto all'interno nell' archivio ZIP allegato al messaggio.

Per ottenere gli indirizzi di posta elettronica a cui inviare la mail infetta, il worm effettua una ricerca nei file con le seguenti estensioni:.WAB, .DBX, .HTM, .HTML, .EML, .TXT.

Il worm falsifica l'indirizzo del mittente nel campo "From:". Può essere 'support@yahoo.com' oppure un qualunque altro indirizzo che il worm rilevi su un sistema infetto.

Sobig.E ha il proprio motore SMTP e contiene una lista di server di posta che utilizza per diffondersi.

Per quanto riguarda la diffusione nella rete locale, Sobig.E enumera le risorse di rete e cerca di localizzare le cartelle di avvio sui computer remoti. Se trova una di queste cartelle, vi copia il proprio file. Il computer remoto viene infettato al successivo riavvio.
