PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 5 - numero 779 di martedì 20 maggio 2003

Worm in velocita'

Rapidità e "data di scadenza", queste le caratteristiche di un nuovo worm che si diffonde via e-mail e sugli share di rete.

Si diffonde rapidamente il nuovo worm, conosciuto con i nomi di "Palyh" e "Mankx", segnalato per la prima volta da Symbolic nel week end scorso.

Non si tratta di un worm distruttivo, ma la sua massiccia diffusione potrebbe creare problemi di "traffico" alle reti; inoltre può essere aggiornato dal suo autore, che potrebbe inserirvi nuove e pericolose funzionalità.
Il worm ha due modalità di propagazione: via e-mail e sugli share di rete.

Una volta installato, il worm si autoinvia a tutti gli indirizzi di posta contenuti nei file con estensione .TXT, .EML, .HTML, .HTM, .DBX, .WAB in tutte le directory sui dischi locali.
Inoltre particolarmente insidioso il fatto che il worm possa propagarsi anche attraverso gli share di rete di Windows; una volta installato "Palyh" enumera tutte le risorse di rete disponibili, se queste sono accessibili, cerca di copiarsi nelle loro cartelle di esecuzione automatica.

Particolarità del worm è inoltre una "data di scadenza" inserita nel suo codice; l'autore ne ha infatti indicato la disattivazione il 31 maggio 2003. A tale data il worm non invierà più e-mail, ma manterrà comunque altre pericolose funzionalità, "prima fra tutte ? secondo gli esperti di Symbolic - la capacità di prelevare ed eseguire codice aggiuntivo da 4 diversi siti web: questa strategia consente a Palyh di costituire un pericoloso "cavallo di troia" sul sistema infetto e di auto-aggiornarsi nel caso in cui l'autore del worm decidesse di inserire nuove funzioni."

Nella diffusione via e-mail, il worm ha due caratteristiche fisse; precisamente il mittente ed il testo. Sono invece variabili il campo "oggetto" ed il nome dell'allegato infetto.

Mittente del messaggio infetto è indicato support@microsoft.com ed il testo fisso dell'e-mail è: "All information is in the attached file.".

I soggetti variano tra i seguenti : Re: My application, Re: Movie, Cool screensaver, Screensaver, Re: My details, Your password, Re: Approved (Ref: 3394-65467), Approved (Ref: 38446-263), Your details.

Il nome dell'allegato infetto, le cui dimensioni variano tra i 49000 e i 54000 byte, è scelto tra: your_details.pif, ref-394755.pif, approved.pif, password.pif, doc_details.pif, screen_temp.pif, screen_doc.pif, movie28.pif, application.pif.
Una volta installato, Palyh effettua una copia di se stesso sul computer infettato e modifica le impostazioni del sistema in modo da attivarsi ad ogni riavvio del computer.
