PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 5 - numero 790 di giovedì 05 giugno 2003

Worm che ritornano

Individuata una nuova variante "a tempo" di Sobig.

Il livello di attenzione nei confronti del worm Sobig, apparso in rete nel mese di maggio, non è destinato ad abbassarsi, anche dopo il raggiungimento della fatidica data del 31 maggio, giorno nel quale il worm è stato programmato per disattivarsi. (Si veda PuntoSicuro n.784).

In rete è stata infatti diffusa una nuova variante di Sobig, anch'essa "a tempo", con scadenza l'8 giugno 2003.
"Al momento - affermano gli esperti di Symbolic - non sappiamo ancora se questo implica che vedremo comparire una variante D nello stesso giorno; se l'autore di queste due varianti e' lo stesso, si e' forse prefisso lo scopo di diventare un "serial virus-writer"? Oppure, si tratta di un gruppo di persone che collaborano o competono tra loro?
Forse il susseguirsi delle due varianti e' semplicemente una conseguenza, o forse no. In ogni caso, il livello di allerta rimarrà elevato fino all'8 giugno. Il consiglio agli utenti e' di controllare che la propria protezione antivirus sia attiva e aggiornata e di trattare le e-mail con allegati con la massima cautela, anche se sembrano provenire da fonti affidabili: se contengono allegati con estensioni eseguibili inusuali (come PIF e SCR, utilizzate da Sobig.C), vanno considerate sospette e analizzate attentamente."

Queste le caratteristiche del worm, che si diffonde via e-mail o tramite le reti locali.
Riguardo al primo metodo di diffusione, il mittente della e-mail infetta è bill@microsoft.com, in altri casi l'indirizzo del mittente è preso in uno dei file presenti sul computer infettato.
Sottolinea Symbolic: "La ricezione di un messaggio infetto da una persona non implica che il mittente sia stato infettato dal worm.
Un utente il cui indirizzo sia stato usato dal worm puo' ricevere messaggi di errori dovuti all'invio di mail ad indirizzi non piu' esistenti o disabilitati. Questi messaggi non causano nessun problema e possono essere ignorati."

I soggetti dei messaggi sono scelti fra: Re: Screensaver; Re: Movie; Re: Submited (004756-3463); Re: 45443-343556; Re: Approved; Approved; Re: Your application; Re: Application.

Il nome dell'allegato e' scelto dalla lista: screensaver.scr; movie.pif; submited.pif; 45443.pif; documents.pif; approved.pif; application.pif; document.pif.

Il testo del messaggio non è variabile e recita "Please see the attached file."
Se l'utente clicca sull'allegato infetto, il worm copia se stesso all'interno del sistema e ne modifica alcuni parametri in modo da essere eseguito tutte le volte che Windows si avvia.
Il worm raccoglie gli indirizzi di posta elettronica, ai quali inviarsi, dai file con le seguenti estensioni: .wab, .dbx, .htm, .html, .eml, .txt.

Per quanto riguarda invece la propagazione attraverso la rete locale, il worm cerca di infettare tutti i computer della rete locale con delle condivisioni accessibili. Per propagarsi cerca di copiarsi all'interno di cartelle predefinite.