PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 5 - numero 727 di mercoledì 26 febbraio 2003

Allarme worm!

Lovgate.C si diffonde via e-mail e colpisce i sistemi Windows. Conosciamone le caratteristiche.

E' elevato il livello di allarme per la diffusione di Lovgate.C, una variante di un worm recentemente individuato.
Il worm si diffonde tramite un allegato di un messaggio di posta elettronica, che ha caratteristiche (soggetto, testo, nome dell'allegato) variabili; l'unico elemento fisso è la dimensione dell'allegato (78846 byte).

Lovgate.C colpisce i sistemi Window; installa nel sistema infetto una componente backdoor che ascolta sulla porta 10168, permettendo ad un eventuale assalitore di eseguire diverse azioni sulla macchina colpita. A quanto appreso da Symbolic, il worm invia informazioni reperite sul computer infettato a due determinati indirizzi di posta elettronica.

Il worm copia se stesso nelle directory condivise utilizzando file con i seguenti nomi: fun.exe, humor.exe, docs.exe, s3msong.exe, midsong.exe, billgt.exe, card.EXE, sETUP.EXE, searchURL.exe, tamagotxi.exe, amster.exe, news_doc.exe, PsPGame.exe, joke.exe, images.exe.

Lovgate.C ha funzioni di keylogging ed e' in grado di memorizzare le informazioni catturate in particolari file.
Il worm inoltre modifica file, in modo tale da essere eseguito ogni volta che l'utente apre un file di testo.
Lovgate.C infine ricerca indirizzi e-mail ai quali inviarsi.

---

www.puntosicuro.it