PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 5 - numero 775 di mercoledì 14 maggio 2003

Nuovo worm che si propaga via e-mail

"Fizzer" può sottrarre dati importanti alla macchina infetta.

Fizzer e' un nuovo worm dell'e-mail piuttosto complesso (segnalato da Symbolic) che ha iniziato la propria diffusione il 9 maggio 2003. Il worm si diffonde via e-mail e nella rete peer-to-peer Kazaa. Fizzer contiene una backdoor IRC, un tool per effettuare attacchi DoS (Denial of Service), un trojan in grado di sottrarre dati dal PC infetto (usa una DLL esterna per fare il Keylogging), un server HTTP e alcuni altri componenti.

Il worm ha una funzionalita' che gli permette di eliminare i moduli residenti di diversi antivirus e puo' auto-aggiornarsi via Internet.
Le sue molteplici capacita' rendono Fizzer potenzialmente pericoloso, specialmente per la possibilita' di sottrarre dati sensibili dalla macchina infetta.

Gli allegati che lo diffondono hanno estensione .EXE, .PIF, .SCR e .COM.
Nomi degli allegati, soggetti e testi delle mail sono scelti a caso da una lista contenuta all'interno del worm.

Gli indirizzi di posta elettronica a cui verra' inviato il messaggio infetto sono raccolti dal Windows Address Book e dalla rubrica di Outlook.
Il codice di Fizzer contiene inoltre delle stringhe di testo in cui l'autore attacca i creatori di software antivirus.

I principali produttori di antivirus hanno rilasciato i file necessari per disinfettare il PC dal worm. E' quindi sempre consigliabile controllare con regolarità le novità dei loro siti.

---

www.puntosicuro.it