PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 3 - numero 414 di giovedì 04 ottobre 2001

Aggiornata la lista delle 20 vulnerabilita' piu' diffuse in Rete

In circolazione un nuovo virus "mascherato" da cleaner per Nimda: Bionet

La Rete è ancora notevolmente esposta agli attacchi di worm e cracker, come ha ribadito Alan Paller, direttore del SANS.
Il SANS Insitute e il National Protection Center (NIPC) hanno, infatti, recentemente rilasciato in rete la lista delle 20 vulnerabilità più importanti, che ancora affliggono i sistemi connessi a Internet.

In questa lista denominata "Twenty Most Critical Internet Security Vulnerabilities" i problemi di sicurezza sono stati suddivisi in tre gruppi: problemi generici (che colpiscono tutti i sistemi), problemi che interessano soltanto le piattaforme Windows e problemi relativi alle piattaforme Unix.

Le password nulle o troppo corte, le porte inutilizzate e lasciate aperte oltre a condivisioni di rete non protette e a vulnerabilità legate ai programmi che gestiscono i rapporti client-server (programmi CGI) sono le voci più frequenti di questa lista.

Nei più comuni attacchi le vulnerabilità utilizzate "sono un esiguo numero", come ha sottolineato Alan Paller, poiché gli autori dei virus si concentrano sulle vulnerabilità più diffuse utilizzando i più noti ed efficaci tool di attacco (come è accaduto per gli worm Code Red e Nimda).

Tramite una e-mail, che in apparenza contiene un cleaner per Nimda, è attualmente in circolazione un nuovo virus: Bionet.
La mail infettante sembra provenire dal noto sito di sicurezza SecurityFocus e dal produttore di antivirus TrendMicro e presenta in allegato un file eseguibile chiamato FIX_NIMDA.exe, che a sua volta contiene il file Readme.txt (effettivamente presente nel cleaner originale di TrendMicro), ma anche il file slide.exe che invece contiene il virus Bionet.

Una volta eseguito il file, Bionet è in grado di aprire nella macchina una backdoor che permette l'accesso e la sottrazione dall'esterno di dati e password.
La falsa mail risulterebbe partita da un servizio di Web-mail tedesco.
Per contrastare l'infezione sarà, quindi, indispensabile verificare sempre l'autenticità del mittente.