PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 569 di martedì 04 giugno 2002

Virus Simile: in circolazione una nuova variante

Il "Trojan" individuato sarebbe in grado di infettare sia i file binari di Windows che quelli di Linux.

E' stato individuato da Symantec alla fine di maggio il virus Simile.D, una nuova variante del virus Simile, che è in grado di infettare sia i file binari di Windows che quelli di Linux.

In base a quanto sottolineato dagli esperti, il virus è capace di utilizzare diverse tecniche di poliformismo e metamorfismo per criptare il proprio codice e variare dinamicamente la propria dimensione.

Con l'adozione di due routine diverse Simile.D è in grado di attaccare i file Portable Executable (PE) di Windows, ma non solo. Come ha specificato Symantec, infatti, il virus " introduce un nuovo meccanismo di infezione anche sulle piattaforme Linux/Intel, infettando i file ELF a 32 bit (un formato binario standard di Unix)".

Anche se i sistemi esposti a una possibile infezione da parte di Simile.D sono Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Me, Linux , la diffusione del virus è al momento abbastanza limitata e gli esperti non lo considerano particolarmente pericoloso, poichè si limiterebbe a far apparire a video alcuni messaggi in date stabilite (17 marzo e 17 settembre su Windows - 17 marzo e 17 maggio su Linux).

Per tutelare la sicurezza degli utenti gli esperti di Symantec raccomandano agli amministratori di sistema di tenere i software aggiornati, installando eventuali patch, di utilizzare password sempre più complesse e di configurare l'email server in modo tale da bloccare i messaggi di posta elettronica che contengano allegati con le estensioni comunemente usate per diffondere virus, quali .vbs, .bat, .exe, .pif e .scr .