PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 635 di venerdì 04 ottobre 2002

Allarme worm!

Segnalati due nuovi worm che si diffondono via e-mail o tramite la condivisione di file in rete. Sistemi Windows a rischio.

Sistemi Windows a rischio: sono infatti bersaglio di due nuovi worm che si stanno diffondendo rapidamente.

Il più pericoloso è Tanatos, conosciuto anche come BugBear, W32/Bugbear, Tanat, W32/Tanat, I-Worm.Tanatos.

Il worm si diffonde tramite posta elettronica o anche attraverso condivisione di file su una rete locale o su sistemi di file-sharing

A quanto riportato da Symbolic, la e-mail con la quale si diffonde il worm Tanatos non ha caratteristiche fisse.
Il soggetto e il corpo del messaggio sono variabili, così come il nome e l'estensione dell'allegato. Unica costante è la dimensione dell'allegato infetto: 50688 byte.

Tanatos mette in serio rischio la sicurezza e la riservatezza dei dati dell'utente colpito, infatti se attivato è in grado di catturare password e username digitati dell'utente.
Questi dati vengono salvati ed inviati ad alcuni indirizzi di posta elettronica che sono crittati all'interno del worm.
Inoltre il worm si autoinvia a tutti gli indirizzi presenti nella rubrica del programma di posta elettronica

Il worm crea una backdoor attraverso la quale è possibile accedere da remoto al sistema infetto ed operare su di esso.

Non utilizza la posta elettronica, ma si diffonde attraverso sui network di condivisione dei file, il worm OpaSoft (denominato anche W32/Opaserv.worm, Worm_Win32_Opasoft, Worm.Win32.Opasoft, Backdoor.OpaSoft).
Il file che contiene il worm e' un PE EXE (portable executable), lungo 28,672 bytes.
OpaSoft si installa nella directory di Windows come "scrsvr.exe".

Una volta installato sul sistema, il worm crea una backdoor e cerca di connettersi al sito internet www.opasoft.com per scaricare aggiornamenti. Il sito è stato ora disattivato.
Come riportato da Symbolic, "tale backdoor utilizza i seguenti data file: "ScrSin.dat" and "ScrSout.dat". La nuova copia del worm viene prelevata con un file dal nome "scrupd.exe" . Quando questo file viene eseguito sostituisce la copia esistente del worm."