PuntoSicuro

## ARTICOLO DI PUNTOSICURO

### Anno 3 - numero 322 di venerdì 20 aprile 2001

# Allarme virus!

***E' stata definita "elevata" la capacita' di diffusione del worm individuato nei giorni scorsi. Come riconoscerlo.***

Diffidate da chi, via e-mail, vi vuole suggerire un metodo infallibile per trovare l'anima gemella! "Want to find your love mates!!! Try this its cool... Looks and Attitude Maching to opposite sex.": questo e' il testo del messaggio dell'e-mail che, come allegato, contiene il file Matcher.exe, un worm scritto in Visual Basic.

"Matcher", la cui presenza e' stata segnalata dall'azienda Symbolic, puo' attaccare i sistemi Windows ed il suo codice e' basato su quello del famigerato virus "Melissa".

Se il destinatario dell'e-mail apre il file Matcher.exe, il virus installa una sua copia nella cartella WindowsSystem e effettua una modifica alla chiave di registro HKEY_LOCAL_MACHINESoftwareMicrosoftWindowsCurrentVersionRun @="C:%winsys%matcher.exe" in modo da venire lanciato ad ogni avvio del sistema.

Seguendo una prassi comune ad altri virus, " Matcher" si autoinvia a tutti gli indirizzi presenti nella rubrica di Outlook mediante un messaggio con soggetto "Matcher" .

E' stato segnalato inoltre che in alcuni casi, il worm ripete la routine di spedizione dei messaggi per ogni indirizzo con cadenza di 1 minuto, generando traffico verso il server di posta.

Matcher effettua anche una modifica al file AUTOEXEC.BAT inserendo l'istruzione:
@echo off
echo from: Bugger
pause

Questo fa sì che, durante l'avvio, il sistema visualizzi la stringa "from: Bugger", rimanendo in attesa della pressione di un tasto per continuare.

Il comunicato di Symbolic precisa che "per rimuovere Matcher, occorre cancellare il file MATCHER.EXE dalla directory WindowsSystem; il file potrebbe risultare bloccato in quanto gia' aperto dal sistema: in quel caso occorrera' riavviare il sistema in modalita' DOS o Provvisoria e procedere all'operazione. Alternativamente, basta rimuovere il valore inserito dal worm nella chiave del registro, riavviare il sistema normalmente e cancellare MATCHER.EXE".



---