PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 531 di lunedì 08 aprile 2002

Rilevato un nuovo mass-mailing worm: W32.Maldal.J

E' in grado di inviare password all'autore del virus. La mail infettante contiene un link in HTML.

E' stato individuato in questi giorni un nuovo virus che si diffonde via email: "W32.Maldal.J".
W32.Maldal.J invia un messaggio di posta elettronica a tutti gli indirizzi presenti nella lista MSN Messenger e nell'address book di Microsoft Outlook, e contiene un link HTML al file "FixerData.exe".

Il messaggio attraverso il quale si diffonde l'infezione ha due differenti versioni:
"I've got this surprise for you ;)
I know what you need at this **** time.

Have fun and don't forget :P YOU KNOW
WHAT I MEAN !
bye"
oppure presenta un testo contenente la seguente frase "We believe that you are infected with W32/ZaCker.Trojan@MM. This High Risk virus allows hackers to control your PC".

Una volta infettata una macchina, questo cavallo di troia copia se stesso nella cartella %Windows%System e sovrascrive al suo contenuto originale un file che contiene il path e il nome del file che contiene il virus.

W32.Maldal.J è, inoltre, in grado di compromettere le impostazioni di sicurezza della macchina colpita e di inviare le password all'autore del virus.

Per ora, il livello di diffusione del worm non mette in allarme gli esperti.
