

## **ARTICOLO DI PUNTOSICURO**

**Anno 5 - numero 744 di venerdì 21 marzo 2003**

# **Attenzione alla posta elettronica!**

*Segnalata la diffusione di un nuovo worm...*

Giunge da Symbolic la segnalazione di un nuovo worm, denominato Ganda (W32/Ganda.A@mm, WORM.SwedenSux, Myzli) che si diffonde tramite uno screen saver, allegato ad un messaggio di posta elettronica.

"Ganda" utilizza un proprio engine SMTP per inviare mail infette a tutti gli indirizzi contenuti all'interno del Microsoft Outlook address book.

Come riconoscere l'e-mail contenete l'allegato infetto?

Il soggetto può essere in lingua inglese o svedese. In lingua inglese i subject utilizzati sono i seguenti: Screensaver advice, Spy pics, GO USA !!!!!, G.W Bush animation, Is USA a UFO?, Is USA always number one?, LINUX, Nazi propaganda?, Catlover, Disgusting propaganda.

Tra i soggetti in lingua svedese vi sono: Olaglig skärmläckar, Rashets eller inte? Hakkors, Go ack ack ack.....,Är USA ett UFO?, Korkad president, Myzli!

L'allegato infetto con estensione SCR ha dimensionedi 62kB (codifica mime). Il nome dell'attachment utilizzato e' sempre corto (ad esempio RG.SCR oppure PW.SCR).

Ogni subject utilizzato e' sempre seguito da uno specifico messaggio contenuto nel testo della mail.

Alcuni dei messaggi utilizzati dal worm tentano di eseguire automaticamente l'allegato infetto al momento dell'apertura della mail.

Il worm tenta, inoltre, di terminare i processi associati a diversi prodotti antivirus.

---

**[www.puntosicuro.it](http://www.puntosicuro.it)**