PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 4 - numero 595 di mercoledì 10 luglio 2002

Allegati pericolosi

Segnalata la diffusione di un nuovo mass-mailing worm.

Non dà tregua il fenomeno del "mass mailing", cioè della diffusione di worm anche non direttamente distruttivi dal punto di vista logico, ma che generano comunque problemi di funzionamento di mailer e sistemi collegati, generando effetti di tipo Denial of Service.

Un nuovo mass-mailing worm, con "elevata" capacità di diffusione, è stato recentemente individuato da Symantec.
Si tratta di Liac.A, un "vermicello" scritto in visual basic, che si propaga attraverso l'allegato di un messaggio di posta elettronica dalle seguenti caratteristiche.

Soggetto: FW:FW: LILAC project video attach
Testo: Things that the govt. dont want you to know
Allegato: LILAC_WHAT_A_WONDERFULNAME.avi.exe

Il file eseguibile, infetto, si cela dietro la falsa estensione ".avi". La dimensione del file eseguibile compresso è di 12,208 bytes (12 K), mentre non compresso è di circa 40K.

Liac.A è in grado di colpire i sistemi Windows 95, Windows 98, Windows NT, Windows 2000, Windows XP, Windows Me.
Quando il worm viene eseguito visualizza il "finto" messaggio di Windows: " Error54: Media Player not installed correctly" e cerca di copiarsi nella directory dei file temporanei di Windows.
Inoltre modifica la chiave di registro
HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun
in modo da essere eseguito ad ogni riavvio del sistema.

A causa di alcuni bachi nel programma, questa operazione non è sempre portata a termine con successo.

Liac.A cerca di utilizzare Microsoft Outlook per autoinviarsi a tutti i contatti presenti nella rubrica di Windows (.wab).
Inoltre modifica la chiave di registro. HKEY_LOCAL_MACHINESOFTWAREMicrosoftWindowsCurrentVersion.

In alcune occasioni il worm avverte l'utente dell'avvenuta "infezione", visualizzando il seguente messaggio: "Your PC is infected with LILAC virus by: xEnOcrAtEs".

---

www.puntosicuro.it