PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 3 - numero 293 di giovedì 08 marzo 2001

Attenti ai virus!

Un nuovo virus si sta diffondendo tramite e-mail, ma non e' l'unica preoccupazione. Gli esperti infatti allertano gli utenti per la persistenza del worm "Hybris".

Pericoli vecchi e nuovi che circolano tramite la posta elettronica.
Un nuovo virus, scritto in Visual Basic, colpisce gli utenti di Outlook. E' stato infatti individuato da F-Secure, azienda produttrice di antivirus, "VBS/Vierika", un virus particolare in quanto la sua attivazione avviene in due fasi.

Il primo componente di "VBS/Vierika" si diffonde tramite l'allegato di un messaggio di posta elettronica la cui vera estensione e' celata mediante un'estensione fittizia (il file "Vierika.JPG.vbs").

Nel caso il mittente apra l'allegato, VBS/Vierika effettua una modifica
al registro di configurazione di Windows, in modo da abbassare il livello di
sicurezza di Internet Explorer.

A questo punto imposta come pagina iniziale per il browser una pagina Web di un sito che contiene la seconda parte del virus. Al momento della connessione, viene lanciato dal sito uno programma che legge la rubrica di Microsoft Outlook e manda un messaggio ad ogni indirizzo.

Queste le caratteristiche dell'e-mail che diffonde il virus:

Da = [Indirizzo dell'utente infetto]
Soggetto = "Vierika is here"
Testo = "Vierika.jpg"
Allegato = ("Vierika.JPG.vbs").

Grazie alla segnalazione degli esperti di F-Secure Corp., il provider presso il quale era ospitata la pagina web che attivava la seconda parte del virus ha provveduto a eliminarla rendendo di fatto inefficace l'azione del worm.

Se pare che Vierika.vbs non avra' una massiccia diffusione; a destare invece piu' serie preoccupazioni e' la persistenza del virus Hybris del quale abbiamo dato notizia nel numero del 10 gennaio 2001.

Secondo il CERT, il centro di coordinamento per la sicurezza informatica della Carnegie Mellon University, la sua diffusione, nel corso dei mesi, e' aumentata.

La difficolta' a bloccare l'"epidemia", questo il parere degli esperti del CERT, consiste nel fatto che i messaggi inviati da Hybris sono anonimi ed e' difficile risalire al mittente; la causa sarebbe individuabile in una non corretta gestione degli open mail relays, server che permettono il passaggio di posta elettronica anche da parte di terzi non autorizzati.
