

ARTICOLO DI PUNTOSICURO

Anno 2 - numero 235 di venerdì 01 dicembre 2000

Allarme virus!

E' stato innalzato il livello di allarme del virus MTX. Attenzione alla posta elettronica.

La notizia giunge da un quotidiano on-line di informatica; un virus, già individuato alla fine di agosto ma del quale si era sottovalutata la capacità di diffusione, si sta dimostrando un serio pericolo per gli utenti della rete.

Il virus, denominato W95.MTX, si diffonde come attachment di posta elettronica e, nel caso l'utente curioso lo apra, può infettare il sistema bloccandone il funzionamento.

"In pericolo" vi sono gli utenti del programma di posta elettronica Outlook su Windows.

Come agisce il virus?

Il virus è costituito da due diverse componenti: un virus e un worm. La componente worm effettua una copia del file Wsock32.dll e, una volta rinominato Wsock32.mtx, lo modifica in modo tale che il virus possa agire.

La componente virus provvede all'invio del virus ogniqualvolta l'utente spedisce un messaggio di posta elettronica.

Come riconoscere il virus?

L'e-mail infetta non ha subject e contiene un file la cui estensione è celata dietro estensioni fittizie. Gli esperti della nota azienda produttrice di antivirus Symantec hanno stilato un elenco dei possibili nomi del file infetto:

I_wanna_see_you.txt.pif, Matrix_screen_saver.scr, Love_letter_for_you.txt.pif, New_playboy_screen_saver.scr, Bill_gates_piece.jpg.pif, Tiazinha.jpg.pif, Feiticeira_nua.jpg.pif, Geocities_free_sites.txt.pif, New_napster_site.txt.pif, Metallica_song.mp3.pif, Anti_cih.exe, Internet_security_forum.doc.pif, Alanis_screen_saver.scr, Reader_digest_letter.txt.pif, Win_\$100_now.doc.pif, Is_linux_good_enough!.txt.pif, Qi_test.exe, Avp_updates.exe, Seicho_no_ie.exe, You_are_fat!.txt.pif, Free_xxx_sites.txt.pif, I_am_sorry.doc.pif, Me_nude.avi.pif, Sorry_about_yesterday.doc.pif, Protect_your_credit.html.pif, Jimi_hendrix.mp3.pif, Hanson.scr, F___ing_with_dogs.scr, Matrix_2_is_out.scr, Zipped_files.exe, Blink_182.mp3.pif.

Gli esperti avvertono che, nel caso sul PC vi siano programmi antivirus attivi, il virus non si attiva, altrimenti inserisce i file le_pack.exe e MTx.exe; quest'ultimo si collega, senza che l'utente possa accorgersene, ad un sito dal quale può aggiornare continuamente il virus.

www.puntosicuro.it