

ARTICOLO DI PUNTOSICURO

Anno 7 - numero 1165 di venerdì 21 gennaio 2005

Worm anti-pornografia

Si spaccia per un tool in grado di eliminare contenuti XXX dal computer, in realtà trasmette una infezione.

Pubblicità

Si cela in un tool di disinfezione di contenuti pornografici il nuovo worm W32/Baba-C, individuato da Sophos. In realtà, aprendo il file allegato al messaggio e-mail con il quale si propaga, l'utente attiva il worm.

Il messaggio, contenente l'allegato infetto, notifica all'utente che sono stati individuati sul suo computer contenuti XXX (magari provenienti dalla visita di siti per adulti) e lo invita ad eliminare le "tracce" mediante il file Evidence Cleaner allegato. In realtà nessun contenuto pornografico è stato individuato e cliccando il file allegato si attiva il W32/Baba-C che si propaga ad altri utenti e apre una backdoor per permettere agli hacker un accesso remoto al computer infettato

L'e-mail infetta ha le seguenti caratteristiche.

Oggetto:

Important! XXX sites found on your computer!

Messaggio:

Windows Evidence Checker has found XXX content on your computer. You can hide your activities with Evidence Cleaner service.

To run Evidence Cleaner click to quick shortcut attached.

Warning! Your copy of Evidence Cleaner will be expired after 7 days. Today you can register for FREE.

Please check attached instructions for more details.

Gli esperti di Sophos ritengono che il worm potrebbe avere una larga diffusione in quanto molte persone sono preoccupate che possa essere scoperta la consultazione, sul loro computer, di siti vietati ai minori.

I contenuti presenti sul sito PuntoSicuro non possono essere utilizzati al fine di addestrare sistemi di intelligenza artificiale.

www.puntosicuro.it