PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 5 - numero 877 di martedì 04 novembre 2003

Attenzione worm!

Un nuovo "vermicello" a caccia di informazioni. Nel frattempo la Guardia di Finanza blocca un worm costato agli utenti, in due giorni, 104 mila euro in connessioni non richieste.

E' stato scoperto e denunciato dal Nucleo Regionale di Polizia Tributaria della Lombardia della Guardia di Finanza l'autore della frode informatica che si nascondeva dietro la diffusione del worm "Zelig". (Si veda PuntoSicuro n.872).

La pericolosità del virus scaturiva dal fatto che, per la prima volta al mondo, sono stati fusi, in un unico programma informatico un worm e un dialer di connessione telefonica all'899.
Alterando le funzionalità del computer infetto, Zelig si autoreplicava tramite e-mail e, contemporaneamente, reimpostava fraudolentemente la connessione ad internet ad un numero di telefono con prefisso 899, a tariffazione maggiorata.

Le statistiche hanno evidenziato, dalle ore 12.00 circa del 24 ottobre alle ore 19.20 circa del 27 ottobre, connessioni illecitamente deviate per un totale di 57794 minuti (a 1,80 euro al minuto), per un totale, quindi di oltre 104mila euro.

Se la truffa non fosse stata prontamente interrotta dall'intervento della Guardia di Finanza, ipotizzando una costanza di collegamenti della stessa frequenza dei primi due giorni, sarebbe stato frodato in un mese un importo pari a circa un milione di euro.

Vinto un worm, ne arriva subito un altro...
Ora è la volta di Mimail, un worm che spia le informazioni riguardanti le finestre aperte di Windows, e cerca di sferrare un attacco DoS (Denial of Service ? Interruzione di Servizio) verso alcuni siti.

Mimail si diffonde tramite email ed è contenuto in un allegato compresso di tipo ZIP nel quale è inserito il componente eseguibile del worm dal nome PHOTOS.JPG.EXE.
L'e-mail infetta è facilmente riconoscibile, in quanto vi sono pochi elementi variabili:
Da: james@[nome del dominio di posta del destinatario]
Soggetto: Re[2]: our private photos [alcuni caratteri scelti a caso]
Messaggio:
Hello Dear!,
Finally i've found possibility to right u, my lovely girl :)
All our photos which i've made at the beach (even when u're without ur bh:))
photos are great! This evening i'll come and we'll make the best SEX :)
Right now enjoy the photos.
Kiss, James.
[alcuni caratteri scelti a caso]
Allegato: photos.zip

Dalle notizie fornite da Symbolic, si apprende che "il worm non utilizza nessun Exploit per auto-eseguirsi. Esso sarà in grado di infettare il PC solo dopo che l'utente abbia decompresso l'allegato e lanciato l'eseguibile."
Se l'allegato viene aperto il worm si installa, modifica dei parametri di sistema e cerca di raccogliere indirizzi e-mail analizzando i file con specifiche estensioni. Gli indirizzi vengono salvati in uno specifico file.

Mimail.C tenta di autoinviarsi agli indirizzi "rubati" e di avviare un attacco DoS (Denial of Service) verso alcuni siti.
Inoltre controlla le finestre di Windows attive e, se esse appartengono a certe applicazioni, Mimail.C raccoglie le informazioni e le salva in uno specifico file.

"Questo file - ha precisato Symbolic - viene inviato a indirizzi e-mail contenuti all'interno del body del worm".

www.puntosicuro.it