PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 5 - numero 887 di martedì 18 novembre 2003

Worm truffa

Una variante del worm MiMail a caccia di numeri di carta di credito.

Il worm Mimail, segnalato all'inizio di novembre, si presenta ora con altri obiettivi in una nuova variante.

Mentre la versione Mimail.C del worm puntava a sferrrare un attacco DoS (Denial of Service) verso alcuni siti e a raccogliere informazioni sulle applicazioni aperte dall'utente; obiettivo della versione Mimail.I sono invece i dati della carta di credito dei destinatari del messaggio e-mail attraverso il quale si diffonde.

Secondo quanto riportato da Symbolic, l'e-mail truffa utilizza un falso indirizzo che sembra provenire dal sistema di pagamenti "Paypal on-line payment service".
Il messaggio richiede l'aggiornamento delle informazioni personali relative al proprio account.
L'email chiede che l'aggiornamento sia effettuato, entro 5 giorni, tramite un modulo allegato (che contiene il virus...) e raccomanda di non inviare informazioni personali via e-mail, in quanto potrebbe non essere sicuro.

le caratteristiche dell'e-mail sono le seguenti:

Da: "PayPal.com" donotreply@paypal.com
Oggetto: YOUR PAYPAL.COM ACCOUNT EXPIRES
Messaggio: Dear PayPal member,
PayPal would like to inform you about some important information regarding your PayPal account. This account, which is associated with this email address will be expiring within five business days. We apologize for any inconvenience that this may cause, but this is occurring because all of our customers are required to update their account settings with their personal information.
We are taking these actions because we are implementing a new security policy on our website to insure everyone's absolute privacy. To avoid any interruption in PayPal services then you will need to run the application that we have sent with this email (see attachment) and follow the instructions. Please do not send your personal information through email, as it will not be as secure.
IMPORTANT! If you do not update your information with our secure application within the next five business days then we will be forced to deactivate your account and you will not be able to use your PayPal account any longer. It is strongly recommended that you take a few minutes out of your busy day and complete this now.
DO NOT REPLY TO THIS MESSAGE VIA EMAIL! This mail is sent by an automated message system and the reply will not be received.
Thank you for using PayPal.

L'**allegato** infetto è www.paypal.com.scr

Se l'allegato viene aperto il worm si installa sul computer, cerca indirizzi e-mail e si autoinvia.
Nel caso un incauto utente compili i campi contenuti nell'allegato, i suoi dati verranno memorizzati in un file ed inviati agli autori del worm...

---

www.puntosicuro.it