PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 6 - numero 1120 di giovedì 11 novembre 2004

Worm aggiornato e...pericoloso

Sfrutta una vulnerabilità non ancora corretta di Internet Explorer.

Abbandonato il tradizionale espediente dell'allegato per diffondersi, le nuove varianti del worm Mydoom operano "da remoto", attivandosi quando l'utente clicca in un link presente in un messaggio infetto che punta verso l'Host che ha inviato la mail infetta.

Symbolic, presentando una descrizione delle due nuove infezioni, precisa che le nuove varianti MyDoom hanno "una backdoor controllata tramite IRC che permette al creatore del worm di trasferire ed eseguire programmi nell' Host infetto."

MyDoom.AG e MyDoom.AH, che sfruttano una vulnerabilità non ancora corretta di Internet Explorer, raccolgono dal computer infetto indirizzi e-mail ai quali inviarsi.
Il mittente della e-mail viene falsificato. Il contenuto della e-mail, secondo le versioni, viene scelto tra:
funny photos :)
hello
hey!
Hi!

Nella versione MyDoom.AG, il corpo della e-mail contiene al suo interno un testo HTML del tipo:
"FREE ADULT VIDEO! SIGN UP NOW!
Look at my homepage with my last webcam photos!"
Il formato del link "infetto" è il seguente:
h**p://:port/

Nella versione MyDoom.AH, il corpo della e-mail contiene al suo interno un testo HTML:

"Congratulations! PayPal has successfully charged $175 to your credit card.
Your order tracking number is A866DEC0, and your item will be shipped
within three business days
To see details please click this
DO NOT REPLY TO THIS MESSAGE VIA EMAIL! This email is being sent by
an automated message system and the reply will not be received."

oppure:
"Hi! I am looking for new friends. I am from Miami, FL.
You can see my with my last webcam photos!"

o messaggi simili.

Il formato del link è il seguente:
h**p://:port/

Le email trasmesse da contengono un header simile a quella autilizzato da alcuni prodotti Antivirus, come ad esempio scanned

for viruses by AMaViS 0.2.1 (http://amavis.org/).
