PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 5 - numero 787 di venerdì 30 maggio 2003

Un worm distruttivo circola in rete

Tenta di cancellare i file presenti sul computer infettato. Le modalità di diffusione.

Sono state rilevate nella serata di mercoledì le prime "infezioni " di Holar, un worm distruttivo che utilizza i tradizionali metodi di diffusione, cioè l'e-mail e le reti P2P di Kazaa (utilizzate per la condivisione di file).

"Il metodo di diffusione di Holar ricorda quello di molti suoi predecessori, con e-mail e allegati dai nomi accattivanti per indurre gli utenti ad eseguirne il codice; - affermano gli esperti di Symbolic - la differenza e' che questo worm, oltre a propagarsi, tenta di cancellare tutti i file dal disco del computer infetto.
L'autore di Holar ha inoltre deciso di conferire un carattere politico al proprio worm: dopo l'eliminazione dei file viene infatti visualizzato un messaggio minaccioso rivolto al presidente USA, George W. Bush, e al popolo ebreo."

Riguardo alla diffusione via e-mail, Holar.H ricava dai file ".htm", ".html", ".txt" e ".dbx" presenti sul disco gli indirizzi a cui spedirsi.
Il messaggio inviato ha caratteristiche variabili.
L'indirizzo del mittente dei messaggi di posta e' ricavato dalle impostazioni predefinite dell'utente.
Nel campo "Oggetto" può essere inserito, ad esempio, uno dei seguenti testi:
"'*< Love Speaks it all >*'", Fw:, Heeeeeeeeeeeeeeey, Hi, I've Got it :), Re:Hi, Who are you??????, WoW But not for NoW.

L'allegato infetto ha nomi variabili, anche il testo dell'e-mail non è fisso, ma scelto tra una decina di messaggi, quali ad esempio:
Hii

Try this great program allowing u to translate 100 languages.
just write a passage in english and chose a language to get the traslation one of my friends used it with his arabian gf and it worked successfully ;)
so , Now we can say ' Love Speaks it All '):

Oppure
Measure your intelligence , the power of your mind and the speed of your reaction by answering several Qs , don't forget to send me your mark. I took 3.5/10 :P Let's see who is more intelligent than the other! Good Luck

In alcuni casi l'e-mail infetta si "maschera", in un messaggio che avverte l'utente di aver inviato file infetti e lo invita a scaricare un file per "disinfettare" il proprio computer:
From: Dispatch@McAfee.com
Subject: Virus Alert !
Dear User, McAfee.com Has recieved an infected message from you .We believe that you are infected with Win32/HaWawi@MM Virus. Please download the attached tool (ToolAv01w32) which will help you to clean your PC. For more information :
*Create an email addressed to virus_research@nai.com.
~U Your name, phone number, address, and email address
~U Operating system
[...]

Per quanto riguarda la diffusione tramite le reti Kazaa, se il computer infetto ha installato il client Kazaa, il worm si copia nella cartella condivisa con nomi scelti in una lista, tra i quali:
Hot_Show.pif, Beauty_VS_Your_FaCe.pif, Endless_life.pif, Hearts_translator.pif, Real_Magic.pif

Utilizzando questi nomi "evocativi", Holar cerca di indurre gli altri utenti a prelevare ed eseguire il file infetto.

Quando Holar.H infetta un sistema, crea due file nella cartella di sistema di Windows e modifica i parametri del sistema in modo da essere eseguito all'avvio di Windows.
Il worm, in determinate condizioni tenta di cancellare tutti i file dal disco C: e visualizza alcuni messaggi, tra i quali uno contro Bush, in diverse finestre di dialogo.
Holar riavvia poi il sistema, ma il danno è fatto.

---

www.puntosicuro.it