ASSOCIAZIONE PICCOLE E MEDIE INDUSTRIE
ADERENTE ALLA CONFAPI

ALLARME VIRUS WORM_BADTRANS.B

WORM_BADTRANS.B

Fascia di rischio: **Media**
Virus tipo: **Worm**
Distruttivo: **No**

Varianti conosciute:

W32/Badtrans-B
BADTRANS.B
W32/Badtrans@MM
W32.Badtrans.B@mm
W32/BadTrans.B-mm

Descrizione:

Questo virus Worm è una variante di WORM_badtrans.a. Si propaga via MAPI32, crea una chiave nel registro del sistema operativo ed arriva con i nomi di file a caso aventi doppia-estensione. Per infettare la macchina, non richiede che il destinatario apra il file allegato al messaggio, ma che legga semplicemente il corpo del messaggio. Come fonte per propagare il virus, usa gli indirizzi presenti nel programma di posta elettronica utilizzato.

Come arriva:

Arriva via e-mail con allegati di questo tipo, ma che possono variare i loro nomi in modo random (casuale):

Pics.ZIP.scr
images.pif
README.TXT.pif
New_Napster_Site.DOC.scr
news_doc.scr
hamster.ZIP.scr
YOU_are_FAT!.TXT.pif
searchURL.scr
SETUP.pif
Card.pif
Me_nude.AVI.pif
Sorry_about_yesterday.DOC.pif
s3msong.MP3.pif
docs.scr
Humor.TXT.pif
fun.pif

Ricordiamo di prestare sempre la massima cautela nell'aprire file allegati di e-mail della cui origine non si sia certi e di esercitare la massima prudenza anche in presenza di allegati provenienti da conoscenti, ma che non erano attesi.

VIA F. LIPPI, 30
25134 BRESCIA
TEL. 030/23076 – FAX 030/2304108
segreteria@api.bs.it

C.F. 80017870173
P.IVA 01548020179

Soluzioni (SOLO PER ESPERTI) in caso di infezione:

1. Cancellare il file CP_25389.NLS nella directory system di windows (%System%\CP_25389.NLS).
2. Avviare l'editor del registro (regedit)
3. Selezionare HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
4. Cancellare la chiave di valore: kernel32
5. Riavviare il sistema.
6. Pulire con un antivirus aggiornato, che riconosca il virus, cancellando tutti i files contenenti WORM_BADTRANS.B.

Supporto & Consulenza Informatica

Dr. Gioachino Roccaro

Tratto dal sito www.antivirus.it ***–Fonte TrenD Micro e PCSELF Osservatorio Virus*** www.pcself.com