APINDUSTRIA
associazione per l'impresa

ALLARME VIRUS W32.Netsky.B@mm

Fascia di rischio:	**Media**	**Virus tipo:**	**Worm**
Distruttivo:	**No**	**Diffusione:**	**e-mail**
Allegato infetto:	**22Kb**	**Varianti in atto:**	**SI**
Sistemi Operativi a rischio:	**Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows XP**		
Sistemi Operativi sicuri:	**Linux, Macintosh, UNIX, Windows 3.x**		
Segnalato anche come	**W32/Netsky.b@MM [McAfee], W32/Netsky.B.worm [Panda], WORM_NETSKY.B [Trend Micro], Moodown.B [F-Secure], I-Worm.Moodown.b [Kaspersky] Varianti: W32.Netsky@mm**		

Descrizione:

worm da posta elettronica che utilizza un proprio SMTP per la spedizione di messaggi infetti a indirizzi recuperati da rubriche di posta elettronica personali o recuperabili in rete da percorsi condivisi.

Come arriva: arriva via e-mail da mittente mascherato/falso, con oggetto una delle seguenti frasi: hi; hello; read it immediately; something for you; warning; information; stolen; fake; unknown.
Il messaggio è una delle seguenti frasi:
anything ok?; what does it mean?; ok; i'm waiting; read the details.; here is the document.; read it immediately!; my hero; here; is that true?; is that your name?; is that your account?; i wait for a reply!; is that from you?; you are a bad writer; I have your password!; something about you!; kill the writer of this document!; i hope it is not true!; your name is wrong; i found this document about you; yes, really?; that is bad; here it is; see you; greetings; stuff about you?; something is going wrong!; information about you; about me; from the chatter; here, the serials; here, the introduction; here, the cheats; that's funny; do you?; reply; take it easy; why?; thats wrong; misc; you earn money; you feel the same; you try to steal; you are bad; something is going wrong; something is fool

Con allegato:

un file di circa 22kb un nome a caso tra i seguenti di formato ZIP:
document; msg; doc; talk; message; creditcard; details; attachment; me; stuff; posting; textfile; concert; information; note; bill; swimmingpool; product; topseller; ps; shower; aboutyou; nomoney; found; story; mails; website; friend; jokes; location; final; release; dinner; ranking; object; mail2; part2; disco; party; misc.
Oppure un file exe con doppia estensione.

Cosa fa:

una volta in esecuzione recupera da file (ad estensione .msg; .oft; .sht; .dbx; .tbb; .adb; .doc; .wab; .asp; .uin; .rtf; .vbs; .html; .htm; .pl; .php; .txt; .eml) locali o in rete indirizzi di posta.
Usa questi indirizzi per spedire un messaggio contenente un file allegato contente il worm e copia se stesso in tutte le cartelle raggiungibili e condivise con vari nomi (doom2.doc.pif sex sex sex sex.doc.exe rfc compilation.doc.exe dictionary.doc.exe win longhorn.doc.exe e.book.doc.exe programming basics.doc.exe how to hack.doc.exe max payne 2.crack.exe e-book.archive.doc.exe virii.scr nero.7.exe eminem - lick my pussy.mp3.pif cool screensaver.scr serial.txt.exe office_crack.exe hardcore porn.jpg.exe angels.pif porno.scr matrix.scr photoshop 9 crack.exe strippoker.exe dolly_buster.jpg.pif winxp_crack.exe). Questa operazione può causare la diffusione di copie di W32.Netsky.B@mm attraverso reti di condivisione file, client , Instant Messaging, cartelle condivise di Windows, o qualsiasi programma che utilizzi cartelle condivise contenenti la dicitura "Share" o "Sharing", "Condivisa". Tra tutte le copie di se stesso crea sotto la cartella di sistema (windows trovata dal worm tramite il nome logico %WinDir%) il file services.exe.

Aggiunge una chiave al registro di sistema HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run con il valore "service"="%Windir%\services.exe -serv". Questo consente al worm di riavviarsi ad ogno segnimento di Windows. Elimina il TaskManager e Explorer dalle chievi di registro HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices

Come eliminarlo:

- Disattivare Opzione Ripristino configurazione di sistema (Windows Me/XP).
- Aggiornare le definizioni dei virus.
- Operare una scansione completa del sistema ed eliminare tutti i file rilevati come W32.Netsky.B@mm.
- Eliminare il valore aggiunto dal worm al Registro di sistema.

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.

Supporto & Consulenza Informatica

Dr. Gioachino Roccaro