APINDUSTRIA
associazione per l'impresa

ALLARME VIRUS "KAMA SUTRA"

Il virus è molto pericoloso, si attiverà ogni giorno 3 del mese (prossima scadenza il 3 febbraio) per distruggere o rendere inutilizzabili files contenenti documenti e dati (".doc", ".xls", ".mdb", ".mde", ".ppt", ".pps", ".zip", ".rar", ".pdf" e ".psd").

Segnalato anche come:
W32/MyWife.d@MM, Kama Sutra, Blackmal.E@mm, Email-Worm.Win32.Nyxem.e, Black worm, Nyxem, MyWife o Tearec.

Come si viene infettati
Veicolo di trasmissione la posta elettronica che ha caratteristiche variabili nell'oggetto, nel testo del messaggio e nel nome dell'allegato, scelti da una lunga lista di opzioni e varianti. Alcuni esempi purtroppo non esaustivi:

Oggetto (uno di questi): *The Best Videoclip Ever, School girl fantasies gone bad, A Great Video, Fuckin Kama Sutra pics, Arab sex DSC-00465.jpg, give me a kiss, *Hot Movie*, Fw: Funny :), Fwd: Photo, Fwd: image.jpg, Fw: Sexy, Re:, Fw:, Fw: Picturs, Fw: DSC-00465.jpg, Word file, eBook.pdf, the file, Part 1 of 6 Video clipe, You Must View This Videoclip!, Miss Lebanon 2006, Re: Sex Video, My photos.*

Corpo del testo (uno di questi): *Note: forwarded message attached, Hot XXX Yahoo Groups, F*ckin Kama Sutra pics, ready to be F*CKED ;), forwarded message attached, VIDEOS! FREE! (US$ 0,00), Please see the file, >> forwarded message, ----- forwarded message -----, i just any one see my photos. It's Free :), how are you?, i send the details, OK ?Fuckin Kama Sutra pics, Note: forwarded message attached. You Must View This Videoclip!.*

Allegato (uno di questi): *007.pif, School.pif, 04.pif, photo.pif, DSC-00465.Pif, image04.pif 677.pif, New_Document_file.pif, eBook.PIF, document.pif, DSC-00465.pIf, Video_part.mim, Attachments00.HQX, Attachments001.BHX, Attachments[001].B64, 3.92315089702606E02.UUE, SeX.mim, Original Message.B64, WinZip.BHX, eBook.Uu, Word_Document.hqx, Word_Document.uu, New Video,zip .sCr, Attachments,zip .SCR, Atta[001],zip .SCR, Clipe,zip .sCr, WinZip,zip .scR, Adults_9,zip .sCR, Photos,zip .sCR, Attachments[001],B64 .sCr, 392315089702606E-02,UUE .scR, SeX,zip .scR, WinZip.zip .sCR, ATT01.zip .sCR, Word.zip .sCR.*

Cosa fa
Il virus raccoglie indirizzi di posta elettronica da vari file locali e in rete come HTM, DBX,EML,MSG,OFT,NWS,VCF,MBX,IMH,TXT,MSF, che userà per spedire messaggi infetti ad altri ignari destinatari. Modifica il registro di sistema della vittima e grazie alle cartelle personali e "documenti recenti" modifica questi file trasformandoli in eseguibili infettanti (purtroppo colpisce anche tutti i computer raggiungibili attraverso condivisioni di rete aperte non protette). Crea anche file eseguibili aventi il seguente nome:

New WinZip File.exe, Zipped Files.exe, movies.exe, WinZip Quick Pick.exe, WINZIP_TMP.exe.

Cerca in rete (tramite le condivisioni aperte su tutto il disco) la presenza dei principali antivirus, li disabilita e ne cancella tutti i files. Ricordiamo che tale modalità operativa non è conforme ai requisiti minimi di sicurezza introdotti con il Dlg 196/2003 (Testo Unico Privacy)

Kama Sutra quando viene attivato su un PC infetto, contatta un sito che offre contatori per pagine Web (sito estraneo all'attacco) e incrementa un contatore, presumibilmente perché in questo modo il padrone del virus può sapere quante vittime ha fatto. Il virus, noto anche come Black worm, Nyxem, MyWife o Tearec, ha così infettato oltre 300.000 sistemi in tutto il mondo (oltre 22.700 in Italia).

Disinfettarsi
Kama Sutra disattiva molti dei più diffusi antivirus, per cui non ci si può fidare che l'antivirus lo debelli. Si consiglia l'uso di un antivirus online, come:

Trend Micro http://it.trendmicro-europe.com/consumer/housecall/housecall_launch.php

Symantec http://security.symantec.com/default.asp?productid=symhome&langid=ie&venid=sym

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.

N.B. Le operazioni consigliate devono essere eseguite da personale esperto. L'associazione non si assume nessuna responsabilità per danni provocati dall'uso delle informazioni fornite.

Supporto & Consulenza Informatica
Dr. Gioachino Roccaro

Aderente a:
Apilombarda
CONFAPI

IT-25134 BRESCIA
Nr. 22156-01

Via F. Lippi, 30
25134 BRESCIA

Tel. 030 23076
Fax 030 2304108
info@apindustria.bs.it
www.apindustria.bs.it