ASSOCIAZIONE PICCOLE E MEDIE INDUSTRIE
ADERENTE ALLA CONFAPI

Spett.le
Azienda Associata

Data l'ondata massiccia d'infezione del virus informatico BUGBEAR nelle due versioni A e B, abbiamo ritenuto opportuno spedire questa comunicazione non via Mailing List, ma come circolare fax. Riteniamo opportuno segnalare alle aziende socie di aumentare il livello di attenzione nell'uso della posta elettronica.
Per ulteriori spiegazioni contattare il servizio Supporto & Consulenza Informatica al numero telefonico 030-23076.

ALLARME VIRUS PE_BUGBEAR.B/A

Fascia di rischio:	**Media**	Distruttivo:	**No**
Virus tipo:	**Worm**	Diffusione:	**e-mail**

Altri Nomi: W32/Kijmo.A-mm, W32.Shamur, W32_BUGBEAR.B

Descrizione

E' una variante del PE_BUGBEAR.A già segnalato precedentemente. Si caratterizza per l'uso della posta elettronica come veicolo d'infezione (usa un proprio programma che sfrutta la porta SMTP) utilizzando i messaggi precedenti (ricevuti/spediti) o la rubrica personale come fonte d'indirizzi. Per rendere più credibile (subdolo) il messaggio, il destinatario viene modificato con un mittente di un precedente messaggio di posta; come testo viene prelevato il testo di un altro messaggio e infine aggiunto un allegato contenente il programma virus (attenzione in questo modo informazioni riservate possono circolare senza il vostro controllo). Ecco perché alcuni hanno rivevuto da Mailing List API un messaggio con il testo non coerente con le informazioni ormai tipiche di questo servizio elettronico e inoltre con le notizie non vengono mai spediti allegati, ma semplicemente i link alle pagine del sito internet API Brescia. Purtroppo solo una lettura attenta del header del messaggio da parte di un esperto può evidenziare il vero mittente.

Come arriva

Arriva via e-mail, con oggetto del messaggio una delle seguenti frasi:
Get 8 FREE issues - no risk! - Hi! - Your News Alert - $150 FREE Bonus! - Re: - Your Gift - New bonus in your cash account - Tools For Your Online Business - Daily Email Reminder – News - free shipping! - its easy - Warning! - SCAM alert!!! - Sponsors needed - new reading - CALL FOR INFORMATION! - 25 merchants and rising – Cows - My eBay ads - empty account - Market Update Report - click on this! – fantastic …ecc..

Con allegato

L'allegato riporta uno dei seguenti nomi: Setup; Card; Docs; news; image; images; pics; resume; photo; video; music; song; data.

L'estensione può essere una delle seguente: EXE, SCR, PIF.

Cosa fa

Una volta aperto l'allegato il computer viene infettato. Il virus cerca tutti gli eseguibili nei dischi di rete non protetti da password (condivisioni di rete non protette) e sul disco locale e gli accoda in programma virus. In particolare infetta (%ProgramFilesDir% corrisponde alla cartella programmi):

- %windows%\scandskw.exe
- %windows%\regedit.exe
- %windows%\mplayer.exe
- %windows%\hh.exe
- %windows%\notepad.exe
- %windows%\winhelp.exe
- %ProgramFilesDir%\Internet Explorer\iexplore.exe
- %ProgramFilesDir%\adobe\acrobat 5.0\reader\acrord32.exe
- %ProgramFilesDir%\WinRAR\WinRAR.exe
- %ProgramFilesDir%\Windows Media Player\mplayer2.exe
- %ProgramFilesDir%\Real\RealPlayer\realplay.exe
- %ProgramFilesDir%\Outlook Express\msimn.exe
- %ProgramFilesDir%\Far\Far.exe
- %ProgramFilesDir%\CuteFTP\cutftp32.exe
- %ProgramFilesDir%\Adobe\Acrobat %ProgramFilesDir%\4.0\Reader\AcroRd32.exe
- %ProgramFilesDir%\ACDSee32\ACDSee32.exe
- %ProgramFilesDir%\MSN Messenger\msnmsgr.exe
- %ProgramFilesDir%\WS_FTP\WS_FTP95.exe
- %ProgramFilesDir%\QuickTime\QuickTimePlayer.exe
- %ProgramFilesDir%\StreamCast\Morpheus\Morpheus.exe
- %ProgramFilesDir%\Zone Labs\ZoneAlarm\ZoneAlarm.exe
- %ProgramFilesDir%\Trillian\Trillian.exe
- %ProgramFilesDir%\Lavasoft\Ad-aware 6\Ad-aware.exe
- %ProgramFilesDir%\AIM95\aim.exe
- %ProgramFilesDir%\Winamp\winamp.exe
- %ProgramFilesDir%\DAP\DAP.exe
- %ProgramFilesDir%\ICQ\Icq.exe
- %ProgramFilesDir%\kazaa\kazaa.exe
- %ProgramFilesDir%\winzip\winzip32.exe

Il virus ferma i principali programmi antivirus e firewall software. Installa nelle cartelle di Esecuzione Automatica (sezione All User) l'eseguibile che infetta il computer al riavvio del PC e crea falsi file di sistema (dll) che non altro che eseguibili (.exe) con estensione (dll).

Come Eliminarlo

Aggiornare il pattern e l'engine del software antivirus. I grandi produttori di software antivirus hanno già catalogato e distribuito gli antidoti necessari. Per la pulizia riavviare il PC in modalità provvisoria. Dopo di ciò sarà possibile cancellare i files di autoinstallazione al riavvio della macchina (%Windows%\All User\Menu Avvio\Programmi\Esecuzione automatica).

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