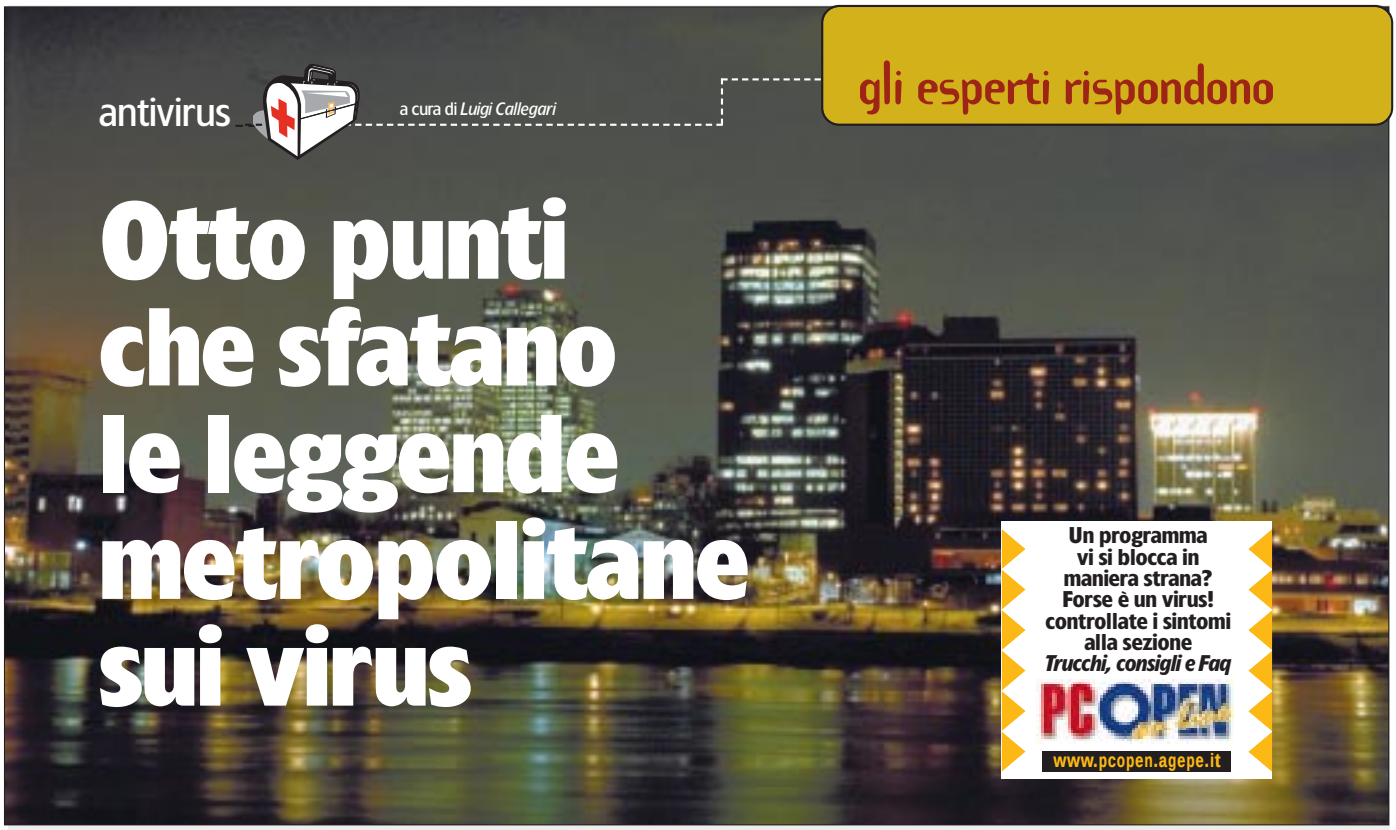
a cura di *Luigi Callegari*

gli esperti rispondono

Otto punti che sfatano le leggende metropolitane sui virus



Sul conto dei virus circola molta disinformazione. Un po' perché sono un argomento ostico e non sempre chi scrive ha la necessaria competenza (vedi stampa quotidiana), un po' perché il mondo dell'informatica è vasto e più complesso di quanto si creda. Abbiamo perciò individuato 8 affermazioni, alcune vere altre false, ma tutte ugualmente significative per conoscere il mondo dei virus e sfatare le sue "leggende metropolitane".

1. I virus attaccano solo file di tipo *.com* e *.exe*
Falso. Questi sono i cosiddetti "file virus", che possono installarsi anche nei file con suffisso *.sys*, ma ne esistono altri. I virus possono installarsi anche nel *boot sector* dei dischi (floppy o hard disk) e in questo caso si chiamano "virus del boot sector), oppure file di documenti o fogli elettronici con suffissi *.rtf, .doc, .xls* e così via. In questo caso si chiamano "macrovirus". Se si usa il programma di estensione dei comandi Shell chiamato *4Dos*, i file virus possono inserirsi anche nei file con suffisso *.btm*, propri di questa applicazione.

2. Posso prendere virus da un file di dati
Falso. Un file che contiene solo dati non viene eseguito, pertanto non può mettere in esecuzione un virus, che è un programma a tutti gli effetti. I macrovirus dei documenti sono collocati nelle macrodefinizioni, ovvero piccoli programmi. In questo caso il file non è più da considerare di "soli dati", ma è un vero e proprio programma, come tale infettabile.

3. Non posso prendere virus dai cookie di Internet
Vero. I cookie sono piccole sequenze di dati che non vengono eseguite come programmi.

4. Posso prendere virus da un file grafico
Falso. Sebbene i normali file grafici dotati di suffissi come *.jpg, .gif, .pcx, .tif* e altri siano dati puri (e come tali non vengono eseguiti e non possono infettare il sistema), va detto però che esistono speciali file grafici distribuiti come file di programma (*.exe*) che includono un programma di visualizzazione che mostra l'immagine contenuta nel file eseguibile stesso. In questo caso, possono eseguire e quindi installare nel sistema il codice di un virus.

5. Un virus può infettare il *Bios* del computer
Vero e falso. I computer Ibm compatibili sin dai modelli con processore 80286 contengono una piccola quantità di memoria (originariamente, 64 bytes, ma oggi possono essere di più) per conservare dati del bios necessari al funzionamento, come l'ora e la data dell'orologio interno, gli hard disk collegati ed altro. Questa memoria non viene eseguita dal processore, solo letta, e quindi non può contenere virus e quindi essere considerata infettata. Però i suoi contenuti possono essere alterati da alcuni virus, per provocare malfunzionamenti appunto nell'orologio e nel dialogo con l'hardware del computer da parte del sistema operativo. Per questo alcuni sistemi antivirus verificano, salvano e possono ripristinare correttamente i contenuti della memoria detta *Cmos* che contiene i dati del bios.

6. Una infezione può essere rivelata dalla alterazione della data di creazione e modifica dei file
Falso. Molti "file virus" quando si installano nel sistema, riscrivono i file in cui si installano, quindi la loro data di creazione o ultima modifica (visibile col comando *Dir* del Dos, oppure col pannello *Proprietà* di Windows 95 e 98) appare modificata e recentissima, più del dovuto. Ma molti altri virus sono abbastanza scaltri da non eseguire queste modifiche, pertanto non necessariamente un file che appare più recente del dovuto (perché noi non lo abbiamo cambiato) contiene un virus, né viceversa un file con data molto vecchia (corrispondente all'installazione o alla data di rilascio del sistema operativo o software) non contiene un file virus.

7. Esistono cure semplici e definitive ai virus
Falso. Sebbene i moderni prodotti antivirus siano ragionevolmente sicuri, non sono a prova di tutti i virus che esistono. Inoltre vanno regolarmente aggiornati ed utilizzati sui dischetti e sui file prelevati da banche dati, cd rom, floppy disk e da Internet. Ma soprattutto è bene controllare file ricevuti da colleghi e amici, per evitare infezioni. Attenzione, non esiste un software antivirus talmente perfetto che, una volta installato, sia una barriera sicura contro ogni tipo di virus presente, passato e futuro.

8. Inibendo l'operazione di scrittura sui file evito infezioni
Falso. Il comando *Dos Attrib*, oppure il pannello *Proprietà del file* di Windows 95 e 98 consentono di inibire la scrittura su di un file. Questo non blocca però l'attacco dei file virus, che non tengono in nessun conto lo stato di scrivibilità del file. ●

Il virus nella posta elettronica: il nuovo pericolo

La posta elettronica è una delle funzioni più pratiche offerte da Internet. Poter spedire testo e file di ogni tipo, a qualsiasi ora nel mondo a costo irrisorio è una grande comodità. Spesso si è verificata sulla e-mail una sorta di terrorismo psicologico, sfruttando impropriamente l'argomento virus. Capita di ricevere messaggi circolari (inviati ad un gran numero di utenti) che invitano a non leggere altri messaggi, perché contengono virus che potrebbero infettare il computer.

Le finte leggende

Si tratta di leggende che abbiamo sfatato più volte. I nostri lettori più fedeli sanno che è impossibile contrarre un virus informatico semplicemente leggendo un messaggio. Infatti, un virus è un programma a tutti gli effetti e deve essere eseguito. Ovvero, deve essere inserito in un file con suffisso *.Com* o *.Exe* nel nome, oppure nel caso dei cosiddetti "macrovirus", in un file *Doc*, *Dot*, *Rtf* e altri che supportino il meccanismo delle macrodefinizioni di operazioni. In ambedue i casi, i virus devono pervenire come file allegati al messaggio ed essere avviati, con l'azione *Risorse* nel caso dei programmi oppure con una videoscrittura nel caso dei macrovirus. In questo caso, bisogna anche confermare l'attivazione dell'esecuzione delle macro nel file, operazione che è potenzialmente pericolosa e quindi intercettata dalle moderne videoscritture (come *Word 97* o *Wordperfect 8*). Se la si nega, il file può risultare illeggibile, ma sicuramente nessun virus di macro può entrare in azione. Se leggiamo semplicemente un messaggio, il programma di posta elettronica (*Outlook*, *Eudora*, *Netscape Messenger eccetera*) lo scandisce passivamente senza eseguire nulla e pertanto non può attivare un virus.

Il bug pericoloso

Tutto questo è vero. Peccato solo che il 3 agosto scorso, *Netscape* e *Microsoft* ammisero ufficialmente che c'era la possibilità di ricevere un virus via e-mail semplicemente aprendo un messaggio di posta elettronica ovvero senza passare per gli allegati ai file. Ciò era causato da un oscuro difetto di programmazione dei loro programmi di gestione E-mail, rilevato e segnalato da tre diverse associazioni indipendenti (*Auscert*, *Ouspg* e *Nt Bugtraq*). In pratica, se si invia un messaggio di posta elettronica con allegato un file dal nome particolarmente lungo e formato in maniera particolare, si verifica un errore inaspettato nel programma di lettura (*Outlook* o *Netscape Messenger*). In questa situazione, e solo in questa, può [illegible] un virus accidentalmente messaggio senza nemmeno eseguire o caricare i file allegati. Sia *Microsoft* che *Netscape* hanno già pubblicato aggiornamenti ai loro programmi di E-mail che sopperiscono a questo difetto e sul cd rom di *Pc Open* trovate proprio l'aggiornamento a *Outlook* italiano.

Con tranquillità

Va detto che, a differenza da quanto pubblicato da molta stampa disinformata, non esiste alcun virus conosciuto che si installi in questo modo. Almeno, secondo i centri di ricerca sui virus di tutto il mondo. Perciò se arriva un messaggio di provenienza sconosciuta, con un file allegato dal file lungo e si verificasse un errore di tipo "buffer underrun" quando si tenta di leggerlo, ci si potrebbe trovare in presenza di un burlone, più che di un virus. Questo non toglie che, conoscendo la perfidia dei creatori di virus, prima o poi qualcuno realizzi questo tipo di virus. Pertanto, è consigliabile installare il "patch" di correzione del problema.

Non tutti ce l'hanno

Si noti che *Outlook* e *Netscape* per *Windows 3.1* non soffrono di questa carenza difensiva nei confronti delle e-mail con file allegati dai nomi difettosi e nemmeno le versioni più aggiornate degli stessi programmi per *Macintosh*. Il programma *Eudora* non risente di questo problema, ma ha invece un "bug" (errore), corretto a partire dalla versione 3.05, che consentirebbe di inserire nel corpo del messaggio un finto riferimento a una pagina Internet. Per questo difetto, non si visita il finto riferimento Internet, ma si avvia un file allegato, dove potrebbe essere inserito un virus. Come sempre, anche con questi "bug" (correggibili, come detto), l'uso attento e coordinato di programmi antivirus e un po' di prudenza nel gestire i file provenienti da fonti sconosciute, consentono di prevenire qualunque infezione. ●

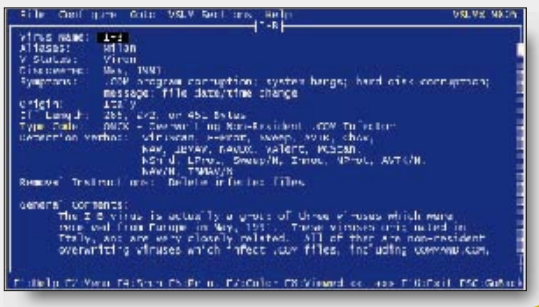
Per conoscere il mondo dei virus e preservare il vostro computer, leggete in rete tutti gli articoli alla sezione *Trucchi, consigli e Faq*

PC OPEN

www.pcopen.agepe.it

I-B: un virus a tempo

Questo virus dimostra che cosa significa "ceppo di virus" e "virus a tempo". Il nome indica infatti un gruppo di tre virus prodotti probabilmente in Italia, dalla stessa mano, viste le caratteristiche molto simili del codice del programma. È a tempo perché entra in azione a un determinato giorno della settimana, scelto casualmente. In questo momento, infetta tutti i file con suffisso *.com* nella directory in cui è collocato. La data e l'ora di questi file vengono aggiornate al momento dell'infezione. Due virus della famiglia *I-B* distruggono anche i primi 160 settori di dati del disco fisso, mentre il terzo tipo blocca il sistema. Per fortuna non è molto pericoloso perché è riconosciuto e distrutto da tutti gli antivirus commerciali.



Il tormentone **Monica continua** sottoforma di **virus**

Gli autori di virus sono persone fantasiose. Una dimostrazione è il virus di macro creato in Italia, a quanto pare, chiamato Lewinsky. Ovviamente ispirato al caso della stagista "amica" di Bill Clinton, questo virus disattiva il sistema di protezione delle infezioni da documenti di Word ed Excel. Come segnalato dai tecnici della Panda Antivirus, se aprendo un documento appare la scritta "Hi Bill, I'm ready for a new BJ" (in italiano, "Ciao Bill, sono pronta per un nuovo rapporto orale") non confermate l'esecuzione delle macro nel documento. Infatti, contiene probabilmente il virus Lewinsky. Il documento pare essere stato diffuso su alcuni siti Internet di materiale pirata (copiato e deprotetto illegalmente) e inviato via e-mail da utenti fittizi a indirizzi postali (mailing list) pubbliche.

Come funziona

A parte lo scherzo di pessimo gusto, ma abbastanza comprensibile visto il clamore del caso, il virus Lewinsky ci dà modo di approfondire la conoscenza del funzionamento di questi virus.
I cosiddetti "macro", ricordiamo, non sono programmi eseguibili ma documenti per Word, Excel e programmi del genere, quindi dotati di suffissi come *.Doc*, *.Tpl*, *.Xls*, *.Rtf* eccetera. La caratteristica è di essere piccoli programmi scritti con il linguaggio di macro di questi programmi. Sono considerati dai programmatori virus facili da realizzare, ma fastidiosi da "depurare". Nel normale funzionamento del personal, le macro consentono di automatizzare alcune procedure. Tra gli esempi di Office abbiamo, ad esempio, un modulo che compila l'intestazione di un fax richiedendo gli input all'utente. Queste operazioni sono programmate appunto con delle sequenze di istruzioni dette in gergo "macro definizioni". Il virus Lewinsky, come moltissimi altri, è formato da una sola macro chiamata appunto come la famosa stagista. Se attivata dall'utente ignaro, inserisce in Word (Excel ed altri) sei funzioni del linguaggio macro: *Auto Open*, *Lewinsky*, *Tools Macro*, *Tools Customize*, *View VB Code* e *File Save As*.
Alcune sono funzioni predefinite del linguaggio macro, che vengono sostituite dal virus per poter compiere interventi impropri sulla vostra macchina. Ad esempio, la nuova *Auto Open* inserisce il virus in tutti i documenti aperti e il file *Normal.dot*, che viene caricato quando si avvia Word (in modo che anche quando si inizia a scrivere e poi si salva, si registra un documento infetto). Il virus Lewinsky è comunque di tipo palese, ben visibile, dato che inserisce il testo "Lewinsky1 Wm97" nella barra di stato di Word e nel titolo dell'applicazione.
Ma non è tutto. Lewinsky è anche un virus a tempo, come molti virus di programma. Infatti, alle ore 12 del giorno 20 di ogni mese, inserisce nel correttore ortografico di Word un riferimento alla voce "the", sostituendola con la frase "This Word Macro Virus was made by WH". Inoltre salva il documento attivo con la password "Lewinskybj", attiva l'assistente di Word e presenta di nuovo la stessa frase. Insomma l'infinito processo a Clinton trova un naturale alleato nei macrovirus.

Rimedi

Il virus è oramai noto e viene riconosciuto dal Panda antivirus e probabilmente dalle versioni aggiornate di altri antivirus. Per evitare il contagio, come sempre, basta non confermare l'attivazione delle macro, che viene richiesta da Word ed Excel quando si apre un qualsiasi documento che le contiene. Ricordarsi di verificare nel menu Strumenti, voce Opzioni, linguetta Standard, che l'opzione "*Protezione da virus macro*" sia attiva, perché altrimenti il software non chiede tale conferma e può essere infettato da un macro virus semplicemente aprendo il documento.
Ricordarsi anche di eseguire sempre la scansione con un antivirus aggiornato di tutti i documenti di fonte incerta. Nel dubbio, non attivare mai le macro e vedere di che tipo di documento si tratta. Questo è particolarmente valido per i documenti che arrivano come allegati in posta elettronica da mittenti sconosciuti (ma anche conosciuti, magari in buona fede).
Vi ricordiamo comunque che, tranne rare eccezioni, i virus non si trasmettono sui messaggi della posta. Non fatevi pertanto spaventare dal potenziale terroristico di questi virus: basta controllare con attenzione i programmi allegati in attachment. Fosse così anche per Monica, Bill e tutta questa sgradevole pantomima. ●

Xuxa, un virus musicale

I virus in genere entrano in azione in modo silenzioso, per non dare nell'occhio. Esistono però delle curiose eccezioni. È il caso della forma *Xuxa*, che pare provenga dall'Argentina, e che suona un motivetto dall'altoparlante interno dei personal computer. Si tratta della colonna sonora della serie televisiva *"El Show de Xuxa"*, la quale andava in onda appunto in Argentina qualche anno fa.
Il virus lo suona tra le 5 e le 6 del pomeriggio, proprio in corrispondenza dell'orario di messa in onda del programma. Oltre a questo, sposta alcuni file sull'hard disk (da cartella a cartella). E, lungo 1728 bytes, infetta i file con suffisso *.com*. Per fortuna può essere intercettato e rimosso da tutti gli antivirus commerciali e di pubblico dominio.