Allarme virus!!!

Prima parte

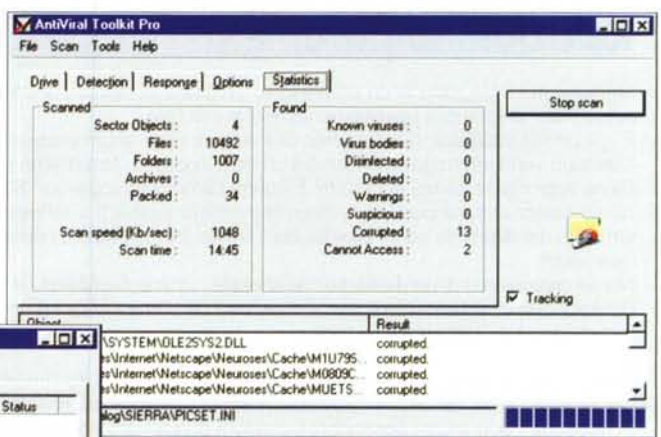
Alcuni anni fa, proprio poco dopo che questa rubrica aveva visto la luce, trattammo su queste pagine del problema dei virus. Tempo ne è passato, e il fenomeno, ben lungi dallo sparire, ha assunto proporzioni planetarie, grazie anche a Internet. E' giusto quindi rispolverare l'argomento, in stile ABC, per dare, a chi poco sa dell'argomento, notizie più certe circa la verità e le leggende che circolano.

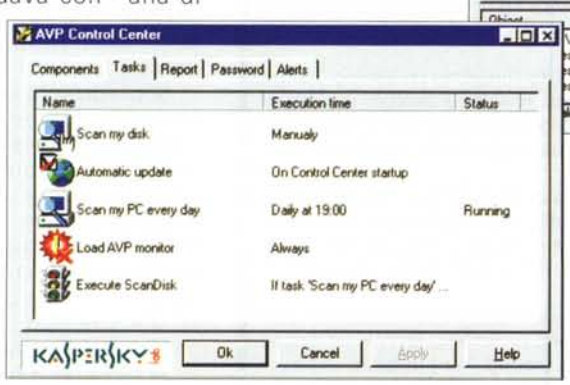
di Raffaello De Masi

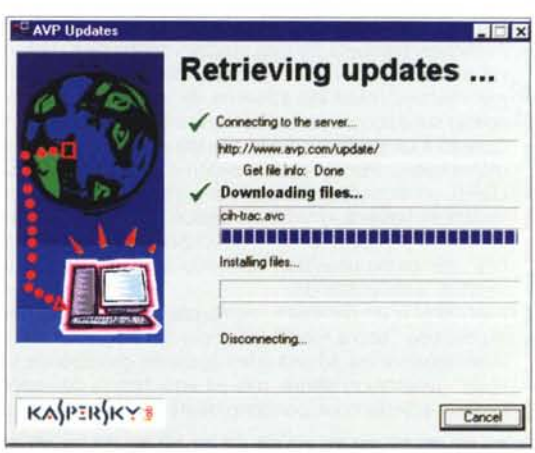
Che bello, ricevere una lettera d'amore! Come si fa a diffidare di chi ti scrive "Ti amo!". L'amore non si può fingere, sconvolge la nostra vita, ci fa sentire più leggeri, ci fa camminare a dieci cm da terra. E magari la profferta d'amore ci arriva da una ragazza che abbiamo assediato con le nostre e-mail! Insomma, non siamo più soli!

E non lo è nemmeno il nostro PC. Una volta perfino le malattie erano più "buone". Se si andava con "una di quelle", poteva accadere di tornarsene con quello che, una volta, era chiamato "un ricordino". Niente di grave, il vecchio farmacista di paese, occhialuto e burbero, ci faceva andare nel retrobottega, profumato di spezie e aromi rari, dove preparava le sue pozioni magiche. E da vecchio uomo di mondo, che ha visto ben di peggio, faceva abbassare le brache al malcapitato "cliente" e redigeva l'immediata diagnosi. Allora il poverino (perché allora ci si vergognava di queste cose, figuratevi che per acquistare dei profilattici, duri come camere d'aria di biciclette, occorreva prendere confidenzialmente il farmacista sotto il braccio, chiedendo con fare ammiccante "una pillola per il mal di testa") prendeva la polverina che l'alchimista gli dava e, con fare circospetto, quasi ladro beccato con la refurtiva, passava per la cassa, sperando che la ragazza non chiedesse ad alta voce che cosa dovesse pagare.

Oggi il neisseria gonorrhoeae non fa paura neppure ai bambini in fasce, i profi-







lattici si comprano a chili nei supermercati, e "mettersi a fare lo scemo" può significare rimetterci la pelle. E' l'evoluzione, nel bene e nel male. Beh, la stessa cosa è avvenuta, più o meno, nel mondo del PC, con un'escalation sempre più dura nella volontà distruttiva e nella pericolosità degli attacchi.

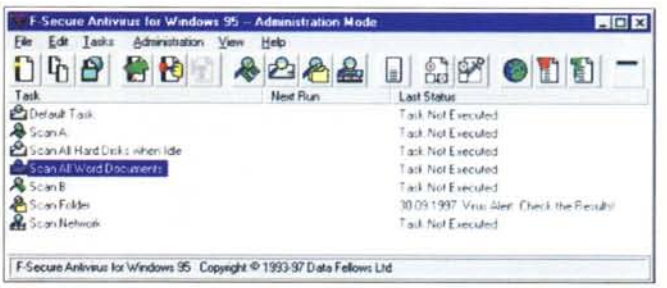
La carta d'identità

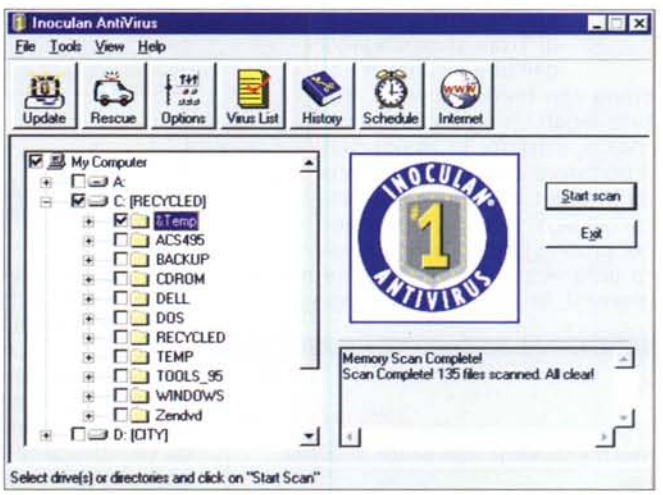
Prima di iniziare, occorre conoscere l'avversario. I virus dei PC non sono creature, sono programmi come gli altri, con la differenza che copiano se stessi su altri per infettarli. Tutto qui, con il fatto poi che non possono partire all'attacco da soli, in quanto per scatenare la virulenza c'è necessità di lanciare il programma infetto. Per essere classificato come virus, un programma deve essere capace di copiare se stesso su un altro programma, o di cancellare parti dei programmi esistenti, semplicemente eseguendo il suo codice.

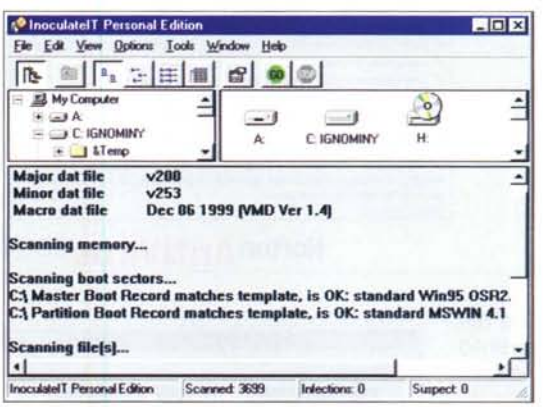
Se volessimo stabilire una definizione di virus potremmo affermare che esso "è un programma capace di replicare se stesso e di copiare parte del suo codice su un altro file, così da modificarlo e/o renderlo inservibile".

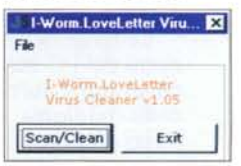
Sembrerebbe, da questa semplice ma completa definizione, che non è possibile un'infezione da virus semplicemente leggendo la posta elettronica o un documento di testo o di wp. Sfortunatamente non è così. La presenza di un linguaggio di programmazione presente nelle applicazioni di Microsoft Office è oggi mezzo diffuso per scrivere virus; "I Love You", tanto per citare uno degli esempi più famosi, era realizzato in questo linguaggio.

Allora, modificando leggermente la definizione precedentemente enunciata, possiamo aggiungere che un virus ha bisogno (come nell'ambiente umano) di un ospite per propagarsi sui dischi di un computer. I virus possono infettare con la tecnica del CTSF (copy to, spread from) file di programmi, programmi su settori di disco, e file che usano macro. La possibilità di autoreplicarsi distingue i virus dai normali programmi, assieme a diverse altre caratteristiche, come quella di risultare invisibili e difficilmente monitorabili durante la loro azione, e questa natura parassitica non è né casuale, né specifica della macchina. In altri termini i virus sono creati da persone che sanno come scrivere programmi per computer, e hanno intenzione di produrre danni o, comunque, fastidio.



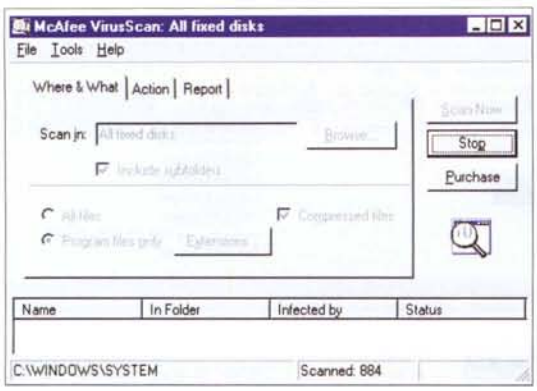






codice specifico per un virus fu scritto e testato nel 1960. Il loro nome deriva da una definizione di A.E. Steiner, docente di cibernetica statunitense, che lo usò nell'84 per rappresentarne l'analogia con un virus biologico, nel senso che è quasi invisibile, duplica se stesso e non può esistere senza un ospite. Col crescere della popolarità della microinformatica, i virus destinati ai PC cominciarono a fare la loro comparsa nella seconda metà degli anni '80, anche se all'inizio avevano, nella maggior parte dei casi, forma di burla o poco più (ricordo il primo che mi beccai, sul Mac, apriva una bella schermata sulla macchina durante le vacanze di Natale, augurava le buone feste e si autocancellava; un virus "buono" insomma!).

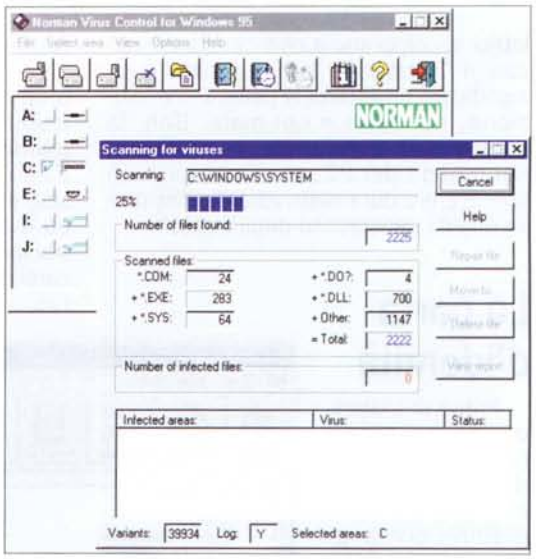
Man mano che le reti intranet e Internet crescevano e si ramificavano, le esigenze di trasmissione di posta elettronica passavano dalla fase di convenienza a quella di necessità. Quale mezzo migliore quindi per trasmettere virus e infezioni? Da qui la comparsa dei Worm, letteralmente verme, essere strisciante, che usa i messaggi di e-mail per



spesso si considera ribelle contro il "sistema".

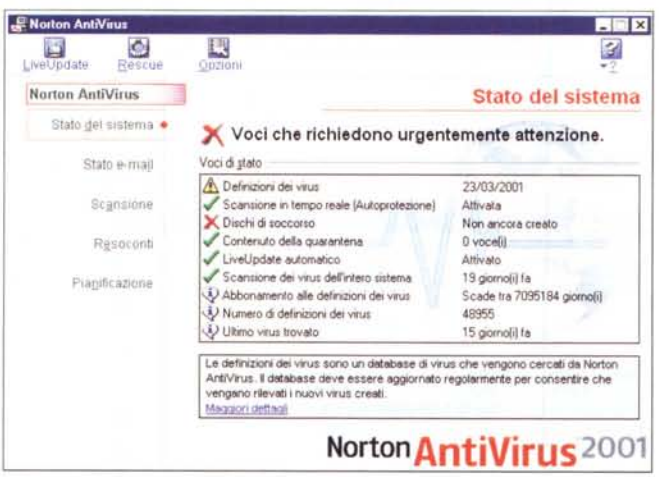
Alla larga dalle infezioni!

Ma come si trasmettono, queste iatture? I virus e i cavalli di Troia si propagano dall'una all'altra macchina con metodi diversi, ma tutti legati, in ogni caso, a un mezzo, l'ospite. In alcuni casi il portatore è un file scaricato da Internet, in altri un dischetto "sporco". Per i worm, invece, proprio perché hanno la loro linfa vitale nei file più che nei programmi, la strada della propagazione del contagio è la trasmissione di posta con i suoi attachment. E questo coinvolge, comprensibilmente, computer legati a reti e LAN. Il discorso, ovviamente, si allarga subito ai file condivisi, in base al principio che è sufficiente che il file sia manipolato in qualche modo da un ospite (si immaginino i newsgroup) per infettarsi, specie in ambienti (parlo sempre dei newsgroup) in cui non esiste possibilità di controllo o affidabilità. Proprio i newsgroup sono sovente la fonte primaria di infezione, e molte persone sono state vittime di nuovi virus e worm, contratti scaricando file messi in biblioteca deliberatamente da vandali.



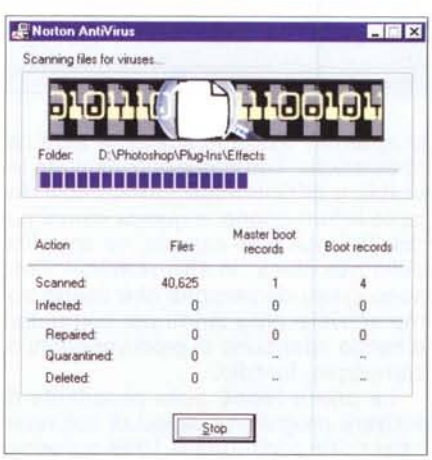
propagarsi. Considerati da alcuni come una sottospecie dei virus, i worm se ne differenziano perché non modificano l'ospite, pur replicandosi e apportando danni di altro tipo.

La terza faccia delle malattie da infezione del PC sono i "cavalli di Troia"; ricavando il nome dal cavallo di legno della mitologia, essi contengono all'interno altri programmi, nocivi o maliziosi, che, una volta trasportati in un'altra macchina, provocano qualunque azione, da semplici (e talora innocui) malfunzionamenti a distruzione di file ed errori irrecuperabili di sistema.



In ogni caso, dal comportarsi come banali ospiti indesiderati a funzionare come vandali assetati di distruzione, i virus vanno combattuti, in tutti i modi. Gli effetti provocati vanno da rallentamento del sistema, all'aumento della frequenza dei crash, all'occupazione della memoria e dello spazio su disco, alla cancellazione di dati. Inoltre si ha un danno indiretto, dovuto al dispendio in denaro per acquistare un buon antivirus e per tenerlo aggiornato.

La RMA Research ha tracciato recentemente l'identikit del realizzatore di virus: maschio, intelligente, età compresa tra i 15 e i 23 anni, istruzione di alto livello, curioso, impegnato in altre attività più o meno fuorilegge, talvolta organizzato in piccoli gruppi (generalmente dalla vita breve). Sostiene di trarre soddisfazione dal senso di sfida sviluppato dalla scrittura del codice, ma

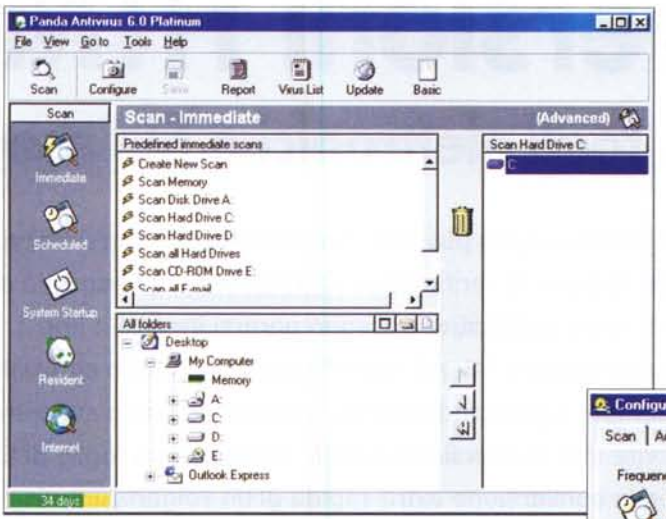


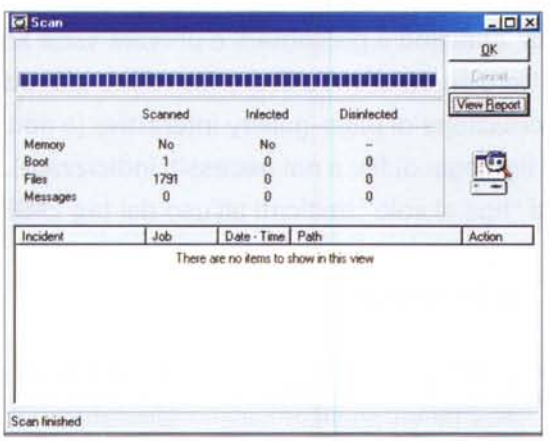
del contagio è la trasmissione di posta con i suoi attachment. E questo coinvolge, comprensibilmente, computer legati a reti e LAN. Il discorso, ovviamente, si allarga subito ai file condivisi, in base al principio che è sufficiente che il file sia manipolato in qualche modo da un ospite (si immaginino i newsgroup) per infettarsi, specie in ambienti (parlo sempre dei newsgroup) in cui non esiste possibilità di controllo o affidabilità. Proprio i newsgroup sono sovente la fonte primaria di infezione, e molte persone sono state vittime di nuovi virus e worm, contratti scaricando file messi in biblioteca deliberatamente da vandali.

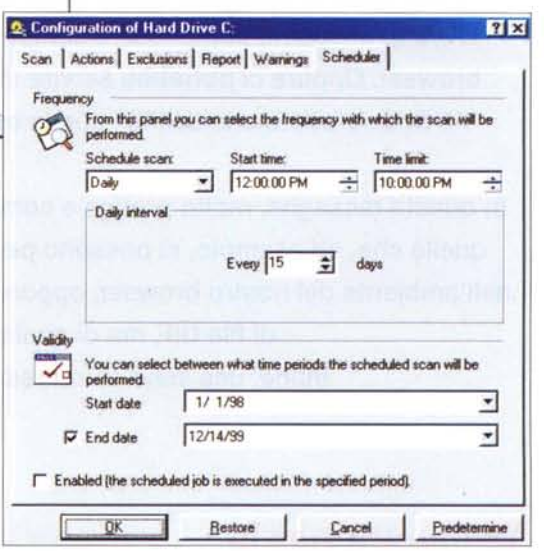
Il fenomeno virus è cresciuto esponenzialmente con la crescita di Internet e lo sviluppo dell'uso della posta elettronica. Prima il contagio era affidato a file infetti che passavano di mano in mano pressoché esclusivamente attraverso floppy e media; il contagio avveniva quindi in maniera lenta e spesso con rami secchi di trasferimento, e i produttori di antivirus erano capaci di mettere a punto un rimedio prima che la situazione divenisse grave. Oggi tutto è cambiato e, specie nel caso dei worm, l'infezione può raggiungere dimensioni planetarie (si ricordino Jerusalem, BackOrifice o I LoveYou, tanto per citarne qualche disastroso esempio) nel giro di qualche giorno. I produttori di virus conoscono quindi questa strada maestra e disegnano prodotti sempre più sofisticati, capaci di trasmettersi in maniera sempre più invisibile e, sovente, senza alcun inter-

vento di operatori esterni. Ecco perché, come si dice, il file attached a un messaggio di e-mail può nascondere comunque un'insidia, e, per assurdo, il file attached più sicuro è un file cancellato.

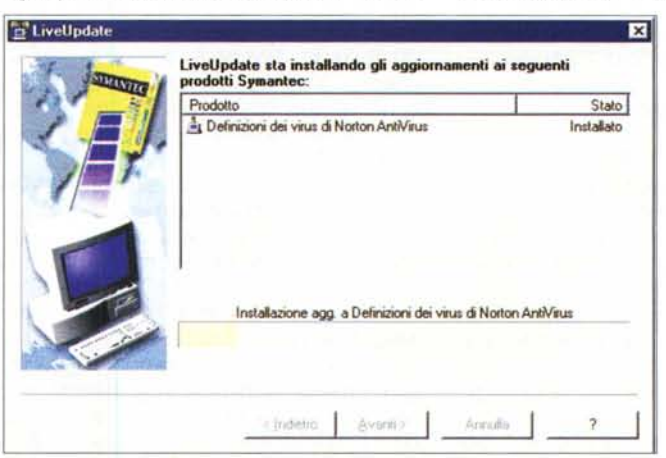
Può un cookie contenere virus? La domanda è legittima, visto anche l'alone di mistero che circola intorno a queste misteriosi oggetti di desiderio. In realtà, i cookie, questi sconosciuti, non sono altro che brevi stringhe o file di testo che sono usati da molti siti quando vengono rivisitati. Ad esempio, quando si personalizzano le pagine di accesso di Yahoo! o Excite, o quando la nostra pagina di posta Web-based ci riconosce, tutto dipende da un cookie contenente le nostre preferenze, la password o il nickname, depositate in questo textfile che viene recuperato e da cui vengono ricavate le personalizzazioni. I cookie sono file ASCII, e quindi non contengono codice di alcun genere (per editarli basta un semplice text editor, anche dei più primitivi); questo elimina, de facto, la possibilità che possano ospitare o trasportare virus. E' teoricamente possibile inserire in un file di questo tipo commenti MIME o UUencoded, ma manca, in queste condizioni, la possibilità di decodificare ed eseguire gli stessi file.







sto non è pensabile, occorre fare in modo di difendersi dagli attacchi (ve la immaginate una persona che resta chiusa in casa per tutta la vita, per evitare di ammalarsi?). Questo non significa che ogni piccolo malfunzionamento del nostro PC sia dovuto a un virus, anzi, nella maggior parte dei casi non lo è. Così sbagliano coloro che, a ogni blocco del sistema o a qualsivoglia evento inspiegabile, gridano "all'untore". Viceversa ci sono in giro virus realizzati in modo tanto raffinato da mascherare perfettamente o quasi la loro presenza. Perciò, come nel corrispondente ambiente umano, evitiamo situazioni a rischio, come aprire senza precauzioni floppy ricevuti da colleghi o studenti, o scaricare senza circospezione materiale di qualsiasi genere senza certa provenienza.



Un antivirus aggiornato giorno per giorno dovrebbe renderci i sonni più tranquilli ma diffidiamo sempre dei file attached alla posta elettronica, anche e sovente soprattutto se ci pervengono da amici o conoscenti. Potrebbero trasmetterci qualche "regalino" magari senza neppure saperlo. Beh, per stavolta chiudiamo. La prossima volta vedremo come fare per prevenire i più gravi problemi e come ridurre al minimo i danni in caso di disastro. E parleremo anche di quel curioso fenomeno noto sotto il nome di hoax e delle altrettanto note Catene (... di S. Antonio!) e di cosa si nasconde dietro! A risentirci!

MC

Conclusioni, per ora...

Beh, adesso conosciamo il nemico; e dobbiamo difendercene. Di come fare parleremo la prossima volta! Per ora possiamo solo dire che il sistema migliore per difendere la nostra macchina è... di tenerla spenta! Ma poiché que-