I virus informatici

Fabio Baccolini, Copyright (c) 2003
E-mail: fabio.baccolini@alice.it

Indice dei capitoli

I. Introduzione ai virus

Cos'è un programma

Prima d'incominciare a parlare dei virus informatici, bisogna spiegare che cosa si intende per programma informatico o più in generale che cosa si intende per programma.

> *Un **programma** è una serie di istruzioni (o se vogliamo di azioni) che devono essere compiute seguendo un preciso ordine affinché si possa conseguire un determinato obiettivo.*

La definizione che ho dato di programma non è vincolata necessariamente al contesto informatico, ma si può applicare tranquillamente alla nostra realtà quotidiana: il programma di un concerto, di una gita, di un corso ricadono tutti nella definizione data.

Proviamo ad impostare un programma per lavare la biancheria. L'obiettivo è quello di trovare una metodologia da seguire affinché riusciamo ad ottenere dei capi lavati perfettamente.

```
PROGRAMMA DI LAVAGGIO
=====================

01. ESAMINA I CAPI DA LAVARE E DIVIDILI IN GRUPPI

    GRUPPO1 -> COTONE BIANCO
    GRUPPO2 -> COTONE COLORATO
    GRUPPO3 -> SINTETICI
    GRUPPO4 -> LANA

02. SCEGLI IL PRIMO GRUPPO DI CAPI DISPONIBILE

03. CARICA LA LAVATRICE

04. AGGIUNGI IL DETERSIVO

05. CHIUDI LA LAVATRICE

06. IMPOSTA LA TEMPERATURA DI LAVAGGIO

    GRUPPO1 (COTONE BIANCO)    -> 90°
    GRUPPO2 (COTONE COLORATO)  -> 60°
    GRUPPO3 (SINTETICI)        -> 40°
    GRUPPO4 (LANA)             -> 30°
```

```
07. IMPOSTA IL PROGRAMMA DI LAVAGGIO

    GRUPPO1 (COTONE BIANCO)    -> 1
    GRUPPO2 (COTONE COLORATO)  -> 2
    GRUPPO3 (SINTETICI)        -> 3
    GRUPPO4 (LANA)             -> 4

08. ATTIVA LA CENTRIFUGA

09. AVVIA LA LAVATRICE

10. ATTENDI LA FINE DEL LAVAGGIO

11. APRI LA LAVATRICE

12. TOGLI LA BIANCHERIA

13. SE CI SONO ALTRI GRUPPI DA LAVARE RIPETI DAL PASSO 2.

14. FINE PROGRAMMA
```

Come prima cosa osserviamo che tutte le istruzioni del programma sono numerate in ordine progressivo. In questo modo ogni istruzione ha un'etichetta che la identifica e la colloca in modo preciso all'interno della sequenza. Ogni programma incomincia con un'istruzione di "inizio programma" e termina con un'istruzione di "fine programma". Alcune istruzioni ci vincolano a prendere una decisione per potere proseguire (***istruzioni condizionali***) e alcune di queste ci offrono delle scelte tra un numero limitato di alternative, come ad esempio la prima istruzione che ci vincola a dividere i capi in quattro gruppi oppure l'istruzione in cui scegliamo la temperatura di lavaggio. L'istruzione **13.** è un'istruzione condizionale vincolata ad una ***istruzione di salto***, serve per evitare che il programma di lavaggio termini se ci sono ancora dei gruppi di capi da lavare.

Un programma informatico è strutturato nello stesso modo dell'esempio: ci sono istruzioni condizionali, istruzioni a scelta multipla, istruzioni di salto, etc. La differenza fondamentale consiste nel linguaggio in cui è formulato: il nostro programma di lavaggio è formulato utilizzando il linguaggio naturale, un programma informatico si esprime attraverso l'uso di un linguaggio matematico. Un'altra differenza è l'esecutore del programma: mentre nel caso del programma di lavaggio possiamo dire d'essere noi ad eseguirlo, un programma informatico viene eseguito da un computer.

Definizione di virus informatico

> *"Un **virus** è un programma informatico replicante, potenzialmente in grado di danneggiare un computer, cancellando dati o causando malfunzionamenti: il danno arrecato è sempre intenzionale. Caratteristica peculiare è che si attacca ad un altro programma, in modo tale che l'esecuzione del programma comporti anche l'esecuzione del virus."*

Innanzi tutto il virus è un **programma informatico** come tutti gli altri e quindi è stato realizzato da un programmatore. Si differenzia da un programma comune per l'obiettivo che si prefigge che coincide con la volontà del programmatore che lo ha realizzato.

L'**obiettivo** di un virus è quello di creare malfunzionamenti nel computer che lo ospita, cancellare o alterare dati e documenti; l'obiettivo di un programma è quello di aiutare l'utente nel realizzare un determinato lavoro.

Un virus è inoltre in grado di **riprodursi**, ossia creare copie di sé stesso, in modo tale da sfruttare il normale scambio di documenti e programmi (attraverso i dischetti o la posta

elettronica) per diffondersi su altri computer. Per fare ciò si **attacca** agli altri programmi, ossia ne modifica il contenuto inserendo al loro interno il proprio codice d'istruzioni, in modo tale che l'esecuzione del programma comporti anche l'esecuzione del virus. Quando il programma modificato verrà eseguito, come prima cosa il virus tenterà d'inserire una copia di se stesso all'interno di un altro programma, ossia di *infettarlo*, in tempi successivi agirà con lo scopo di arrecare danni al computer che lo ospita. Dal momento che uno degli obiettivi del virus è quello di diffondersi senza essere scoperto, può tentare di agire utilizzando due diversi tipi di tecniche: rimanere inattivo per lungo tempo limitandosi a replicarsi e creare ingenti danni in un solo colpo, spesso in coincidenza con determinate date (*bomba a tempo – time bomb*) oppure causare, giorno dopo giorno, lievi danni ai documenti o piccoli malfunzionamenti che però alla lunga, sommandosi, diventano consistenti.

Alcune cose importanti occorre puntualizzare:

- un virus non è in grado di danneggiare in alcun modo l'*hardware* del computer, ossia i dispositivi elettronici;
- un virus può danneggiare dati e documenti, nel senso che può cancellarli o alterare il loro contenuto;
- può danneggiare i programmi, causare blocchi o malfunzionamenti rendendo talvolta il computer inutilizzabile.

Ciò può rendere necessario l'intervento di un tecnico per eliminare il virus ed eventualmente ricaricare il sistema operativo ("Windows", per intenderci) assieme ai programmi (Microsoft Word, Excel, Access, Power Point) e ai dati. Una volta terminato questo intervento il computer riprende a funzionare in modo corretto. Non è possibile in alcun modo ricaricare i dati e i documenti se non è disponibile una copia di salvataggio.

> *Occorre abituarsi ad effettuare periodicamente delle copie di sicurezza dei propri dati (**backup**) per evitare che un virus, un guasto del computer o un errore dell'utente possano irrimediabilmente compromettere il lavoro di mesi o talvolta anche di anni.*

Molte persone non sanno che i propri dati sono contenuti dentro ad un dispositivo che si chiama ***disco fisso*** o ***hard disk***, a sua volta alloggiato all'interno del computer. Se questo componente si guasta (e normalmente capita di frequente perché è un dispositivo estremamente delicato), non si può fare altro che sostituirlo con uno nuovo. Il computer ritorna come nuovo, ma i nostri documenti vanno a finire nella spazzatura assieme al disco rotto.

Esistono in commercio molte unità in grado di effettuare il salvataggio dei dati. Si parte dai floppy disk, per passare a delle unità a dischetti di capacità maggiore (come gli ZIP100 della Iomega o gli LS120). Attualmente si sta diffondendo molto l'uso del masterizzatore, si tratta di un'unità fatta in modo simile al lettore per i cd-rom, ma a differenza di questo che è soltanto in grado di leggerli, il masterizzatore può anche inciderli. La sua diffusione è legata soprattutto al fatto che i cd-rom vergini (cioè quelli non ancora incisi) costano poche migliaia di vecchie lire ed hanno una capacità pari a quella di 500 floppy disk. I masterizzatori di ultima generazione sono in grado anche di scrivere su dei supporti speciali (chiamati cd-riscrivibili) che possono venire incisi e poi cancellati per un numero praticamente illimitato di volte, a differenza dei cd-rom classici che possono venire incisi una volta soltanto.

Quando è necessario salvare grosse moli di dati, si possono utilizzare delle unità a nastro che hanno il pregio di avere un'altissima capacità (equivalente a 35-70 cd, a seconda del tipo di nastro) ma il difetto di essere estremamente lente e costose.

Paragone tra i virus biologici e i virus informatici

Il motivo per cui i virus informatici sono stati chiamati "virus" è perché il loro comportamento risulta abbastanza simile agli omologhi biologici.

- Un virus informatico sfrutta un programma "ospite" per diffondersi e causare danni, allo stesso modo di un virus biologico che sfrutta le cellule dell'organismo ospite.
- Un virus informatico modifica un programma inserendo al suo interno il proprio codice di istruzioni, un virus biologico modifica il DNA della cellula che lo ospita.
- Entrambi sono in grado di diffondersi ed infettare altri "individui".
- Entrambi sono pericolosi.
- Abbiamo detto che un virus informatico può rimanere "latente" per svariato tempo, è l'equivalente del periodo di incubazione del virus biologico.

Un esempio di virus

Per fare capire meglio il meccanismo di azione di un virus informatico, ho pensato di costruire un virus per il nostro programma di lavaggio. Ricordiamo che l'obiettivo del programma è quello di offrire un bucato perfetto a chi lo utilizza, naturalmente l'obiettivo del virus è quello di danneggiare il bucato creando ad esempio delle macchie. Il meccanismo d'azione di questo virus che chiamerò ***virus primo d'aprile*** (e ne capirete presto il motivo) è identico a quello di molti dei virus attualmente in circolazione; la differenza consiste nel fatto che è scritto utilizzando il linguaggio naturale.

Prima di incominciare a presentare il virus primo d'aprile occorre fare una piccola premessa: affinché un virus possa incominciare a diffondersi bisogna che il programmatore, in principio, lo sparga in giro di persona. Quando la diffusione ha raggiunto un minimo di consistenza allora la catena può continuare da sola e il virus diventa per così dire autonomo. Per fare un esempio, se vogliamo che un'erba infestante si diffonda all'interno di un certo territorio, occorre che in principio andiamo in giro a spargere delle sementi.

Noi ipotizziamo che queste "sementi" siano state già sparse e che una di queste abbia, in un qualche modo, raggiunto il computer che ospita il programma di lavaggio. Quindi il virus è entrato dentro, ha infettato il programma di lavaggio e vuole tentare di infettare altri programmi: vediamo come lo ha modificato per inserire al suo interno il codice virale. Come prima azione ha creato un punto di inserimento: l'istruzione **02.** è stata sostituita con un'istruzione di salto al passo **15.**, quindi il virus ha ricopiato il proprio codice accodandolo alla fine, ricreato come passo **17.** l'istruzione che c'era in origine al passo **02.** e infine ha inserito un punto di ritorno al passo **03.**, in modo tale da fare riprendere normalmente l'esecuzione del programma. Il risultato è il seguente:

```
PROGRAMMA DI LAVAGGIO INFETTATO DAL VIRUS 1° APRILE
===================================================

01. ESAMINA I CAPI DA LAVARE E DIVIDILI IN GRUPPI

    GRUPPO1 -> COTONE BIANCO
    GRUPPO2 -> COTONE COLORATO
    GRUPPO3 -> SINTETICI
    GRUPPO4 -> LANA

02. VIRUS: SALTA AL PASSO 15.

03. CARICA LA LAVATRICE

04. AGGIUNGI IL DETERSIVO

05. CHIUDI LA LAVATRICE

06. IMPOSTA LA TEMPERATURA DI LAVAGGIO
```

```
    GRUPPO1 (COTONE BIANCO)    -> 90°
    GRUPPO2 (COTONE COLORATO)  -> 60°
    GRUPPO3 (SINTETICI)        -> 40°
    GRUPPO4 (LANA)             -> 30°

07. IMPOSTA IL PROGRAMMA DI LAVAGGIO

    GRUPPO1 (COTONE BIANCO)    -> 1
    GRUPPO2 (COTONE COLORATO)  -> 2
    GRUPPO3 (SINTETICI)        -> 3
    GRUPPO4 (LANA)             -> 4

08. ATTIVA LA CENTRIFUGA

09. AVVIA LA LAVATRICE

10. ATTENDI LA FINE DEL LAVAGGIO

11. APRI LA LAVATRICE

12. TOGLI LA BIANCHERIA

13. SE CI SONO ALTRI GRUPPI DA LAVARE RIPETI DAL PASSO 2.

14. FINE PROGRAMMA

15. VIRUS: SE NEL COMPUTER C'E' UN ALTRO PROGRAMMA DI LAVAGGIO
    NON ANCORA INFETTATO AGGIUNGI IL CODICE DEL VIRUS

16. VIRUS: SE OGGI E' IL 1° DI APRILE MISCHIA, SE POSSIBILE, IL
    COTONE BIANCO COL COTONE COLORATO

17. VIRUS: SCEGLI IL PRIMO GRUPPO DI CAPI DISPONIBILE

18. VIRUS: SALTA AL PASSO 03.
```

Il programma così modificato si comporta normalmente quasi tutti i giorni dell'anno eccetto che, ad ogni esecuzione, tenta di aggiungere il proprio codice ad altri programmi analoghi di lavaggio; il primo di aprile, però, produce un danno mischiando il cotone bianco col cotone colorato. Da osservare che al punto **15.** si ci arriva solo attraverso l'istruzione **02.** di salto, infatti quando l'esecuzione arriva al punto **14.** il programma termina.

La diffusione del virus su altri computer avviene nel momento in cui l'utente, ignaro dell'infezione, distribuisce delle copie del proprio programma di lavaggio ad amici o ad altre lavanderie. Queste caricano sui loro computer il programma infetto e l'infezione attacca anche i loro programmi di lavaggio. La catena in questo modo continua.

Il sistema operativo

Il sistema operativo è un particolare tipo di software che ha il compito di gestire i dispositivi elettronici che compongono il computer (*periferiche interne*) e tutti gli accessori esterni come monitor, mouse, tastiera, stampante, scanner (*periferiche esterne*). Perché il computer possa funzionare occorre che tutti questi dispositivi agiscano in sincronia e svolgano ciascuno le proprie funzioni quando è il loro turno. Per avere un'idea dell'importanza della funzione svolta dal sistema operativo, pensate a che cosa accadrebbe se gli automobilisti smettessero di rispettare il codice della strada e facessero ciascuno a modo suo.

I programmi possono girare perché c'è il sistema operativo che fa funzionare tutti i dispositivi elettronici in modo ottimale. Windows 95, 98, ME, NT, 2000 sono sistemi operativi prodotti dalla Microsoft; tra questi, Windows NT e Windows 2000 vengono utilizzati quasi

esclusivamente in ambito aziendale. Sempre in ambito aziendale vengono ampiamente utilizzati anche dei sistemi operativi non Microsoft: Linux ne è un esempio. Si tratta di un sistema operativo gratuito, gestito da un'organizzazione internazionale non a fine di lucro, fondata da Linus Torvalds, e viene utilizzato principalmente sui server in rete per le sue doti di eccezionale stabilità. Aggiungiamo infine a questa lista i sistemi operativi Mac OS che funzionano esclusivamente sui computer Macintosh.

I programmi vengono progettati in funzione del sistema operativo che li dovrà ospitare. Questo significa che un programma progettato per Windows non funzionerà su un computer che utilizza Linux e viceversa. La stessa cosa vale per i virus informatici: un virus funziona sul sistema operativo per il quale è stato progettato, i virus in grado di diffondersi su diversi tipi di sistemi operativi esistono ma sono più rari.

Come si prende un virus

Un virus è un programma informatico, affinché possa diffondersi e infettare un computer occorre che il programma infetto venga mandato in esecuzione. Devono quindi verificarsi due situazioni ben precise:

- una terza persona mi ha dato un programma infetto,
- ho mandato in esecuzione il programma almeno una volta.

I programmi vengono distribuiti attraverso i dischetti, i cd-rom e la posta elettronica. Si possono anche scaricare dai siti Web. Se utilizzo un dischetto su un computer con un virus (a scuola o sul lavoro per esempio), il dischetto può venire a sua volta infettato. Se successivamente utilizzo il dischetto a casa, l'infezione passa sul mio computer. L'infezione non si può trasmettere sopra un supporto che non può essere scritto, come ad esempio un cd-rom o un floppy che che è stato protetto da scrittura con l'apposita linguetta. Infatti, il virus per infettare un programma lo deve modificare e quindi deve andare a scrivere sul supporto dove il programma è memorizzato. Riguardo ai cd-rom, occorre precisare che può accadere invece che vi vengano memorizzati sopra dei programmi già infetti, anche all'insaputa di chi lo masterizza; questa situazione si può per esempio verificare se scarichiamo da Internet un programma infetto e poi lo masterizziamo su cd.

Facciamo alcuni esempi per chiarire alcune situazioni di possibile contagio. Se mi viene dato un dischetto infetto fino a quando non lo utilizzo sono al sicuro. Se su questo dischetto ci sono 3 programmi (es. lavaggio1, lavaggio2, lavaggio3) di cui solo lavaggio3 è infetto, l'infezione comincerà a propagarsi nel momento in cui vado ad utilizzare, per la prima volta, lavaggio3. Con ogni probabilità, il programma infetto contaminerà, per primi, i due sani per poi passare agli altri programmi presenti sul disco rigido del computer.

Un virus può infettate solo i programmi o anche i documenti e le pagine Web?

Esistono alcuni tipi di documenti (per esempio quelli fatti con Microsoft Word, Excel, Access, Power Point) che al loro interno possono ospitare dei piccoli programmi che servono per automatizzare alcune operazioni (le cosiddette macro). Tali tipi di documenti sono quindi attaccabili dai virus.

> *I virus che infettato i documenti realizzati con Word ed Excel sono **diffusissimi**, perché esiste un fortissimo scambio tra aziende, uffici, enti pubblici e privati di documenti realizzati con i prodotti Microsoft. Fortunatamente, però, i virus delle macro non sono molto pericolosi e si eliminano con facilità.*

Altri tipi di file che contengono programmi sono gli ***screen saver*** (i salva-schermo), ossia quelle immagini che scorrono sul nostro computer automaticamente, dopo che questo viene

lasciato inattivo per un certo periodo di tempo. Anche le pagine Internet possono ospitare al loro interno dei programmi, utilizzati per colorare la pagina con effetti grafici (***programmi Java, Javascript e controlli ActiveX***). Quindi teoricamente si possono prendere dei virus anche navigando in Internet, anche se si tratta di un'eventualità rara, perché i gestori dei siti Web controllano quotidianamente il contenuto dei loro siti. Chi gestisce un sito di una certa importanza, verifica costantemente il materiale che viene pubblicato e si accerta che non vi siano virus entrati nel sistema: ne va dell'immagine del sito stesso. Navigando su siti pirati, a carattere pornografico oppure su siti che contengono "materiale spazzatura", non si sa in che cosa ci si può imbattere: la probabilità di prendere un virus è molto alta.

Le immagini (bmp, gif, jpg, tif), i suoni (mid, mp3, wav), i filmati (avi, mpg), i documenti di Acrobat (pdf) e di puro testo (rtf, txt) invece non contengono codice eseguibile e quindi non sono fonti di diffusione di virus. Può capitare che un virus riuscito male vada per sbaglio ad attaccare un'immagine o un suono. In questo caso non c'è nessun pericolo di prendere il virus, perché l'immagine non viene eseguita a differenza di un programma, al più succederà che una parte di essa risulterà non leggibile.

Boot sector virus

Nel momento in cui viene acceso, il computer va a leggere il primo settore del disco rigido ed esegue le informazioni in esso contenute che in pratica sono le istruzioni per avviare il sistema operativo. Esistono alcuni tipi di virus, chiamati ***boot sector virus***, che si inseriscono nel primo settore del disco (denominato *boot sector*, ossia settore di avvio). Anche un floppy possiede un boot sector che può essere programmato per potere avviare il computer da dischetto qualora non sia possibile farlo normalmente. Se in fase d'accensione è inserito un floppy, il computer va a leggere e ad eseguire il suo *boot sector*, dando la precedenza a quello del disco rigido; qualora nel floppy sia presente un *boot sector virus* questo viene mandato in esecuzione. Lasciare quindi un dischetto inserito all'avvio del computer può essere un modo per prendersi un virus.

Riguardo ai boot sector virus occorre precisare che mentre fino ad alcuni anni fa erano diffusissimi, attualmente stanno diventando sempre più rari.

I virus della posta elettronica

I virus di posta elettronica si diffondono inviando delle e-mail con allegato una copia di se stessi; questa operazione viene svolta in maniera completamente invisibile agli occhi dello sventurato utente che ha contratto il virus. Il destinatario della e-mail viene scelto di norma dalla nostra rubrica personale oppure viene "rubato" dalle e-mail che spediamo. L'oggetto e il corpo del messaggio vengono costruiti dal virus, talvolta anche utilizzando delle frasi prese dai nostri documenti personali; in alcuni casi sono invece vuoti. L'allegato infetto può avere svariati nomi, spesso anche molto originali (es. love_letter_for_you). La persona che riceve la nostra lettera apre l'allegato (che ritiene sicuro perché proviene da un amico) e prende il virus. Normalmente l'apertura dell'allegato non produce alcun effetto visivo; in alcuni casi viene visualizzato un falso messaggio di errore che ci informa che non è stato possibile aprire l'allegato, perché danneggiato. La persona si interroga per qualche secondo su questa cosa e poi prosegue con le proprie attività; nel frattempo il virus è entrato nel sistema ed è operativo. Alcuni virus sono diventati storici perché i loro allegati producevano effetti grafici molto accattivanti: l'apertura dell'allegato del virus Happy99 simulava un'esplosione di fuochi artificiali.

A quanto detto aggiungiamo che alcune versioni di Internet Explorer possiedono delle imperfezioni (in gergo tecnico *bug* che tradotto letteralmente significa insetto) che vengono sfruttate per causare l'esecuzione automatica dell'allegato di posta. In pratica, in alcune condizioni particolari, il virus è in grado d'infettare il sistema in modo automatico anche senza che l'utente apra l'allegato infetto.

La diffusione di questi tipi di virus è molto alta proprio perché la fonte da cui si riceve il virus è in genere ritenuta sicura.

Occorre non fare confusione tra i virus di posta elettronica e i documenti di Word e di Excel che spesso spediamo come allegati di posta elettronica, nell'ambito degli scambi di documenti e informazioni che avvengono quotidianamente. Anche questi possono contenere dei virus (quasi sempre all'insaputa del mittente), la differenza consiste nel fatto che siamo noi ad allegare il documento alla lettera.

Riassunto sui vari tipi di virus

- **Virus che attacca i programmi (file virus)**: il codice del virus viene eseguito all'avvio del programma.
- **Virus che attacca il settore di avvio del computer (boot sector virus)**: il virus viene eseguito ad ogni accensione.
- **Macro virus**: infetta determinati tipi di documenti, in particolare quelli fatti con Word ed Excel. L'apertura del documento comporta l'esecuzione del virus.
- **Virus di rete (network virus)**: utilizza i protocolli di rete o la posta elettronica per diffondersi. Fanno parte di questa categoria anche i virus che attaccano le pagine Web.
- **Virus combinato (combo)**: utilizza diverse modalità d'infezione.

Tabella di pericolosità dei virus

Tipo di virus	*Pericolosità*	*Rischio di prenderlo*
Virus dei programmi	Alta	Basso
Virus del settore d'avvio	Alta	Molto basso
Virus delle macro	Bassa	Alto
Virus di posta elettronica	Alta	Molto alto
Virus delle pagine Web	Alta	Basso (*)

(*) Dipende dai siti dove si naviga: il rischio diventa altissimo nei siti pirati o a carattere pornografico.

Antivirus

Per *antivirus* si intende un programma in grado di riconoscere e rimuovere i virus presenti sul computer. Un antivirus per potere essere efficace deve essere aggiornato, ossia occorre inserire le informazioni sui virus recenti. Tale operazione viene effettuata attraverso Internet dal programma stesso, premendo un apposito bottone mentre siamo connessi. L'antivirus può essere utilizzato in due modi diversi: si può mandare in esecuzione manualmente per controllare dei file sospetti oppure può essere impostato in modo tale da essere sempre attivo. Personalmente consiglio la modalità “sempre attiva”, perché così il computer viene mantenuto costantemente sotto controllo: in questo caso l'antivirus esegue una vera e propria attività di prevenzione, analizzando tutto ciò che passa per il computer e bloccando tutti i file sospetti. Tutti gli antivirus in commercio utilizzano la modalità “sempre attiva” come modalità predefinita di funzionamento e offrono la possibilità di avviare la “scansione” manuale dei file. Pertanto, in fase d'installazione dell'antivirus, non dovrete fare altro che confermare le scelte che vi verranno proposte, per ottenere un antivirus operativo in tutte le sue potenzialità.

La capacità distruttiva di un virus

- **Virus totalmente innocui**: si propagano nel computer occupando spazio, ma non producono effetti distruttivi.
- **Virus non pericolosi**: generano saltuariamente effetti grafici o sonori, come ad esempio la classica pallina che rimbalza sullo schermo.
- **Pericolosi**: causano malfunzionamenti del computer, modificano o cancellano i documenti da noi creati.
- **Altamente pericolosi**: causano il completo inutilizzo del computer o la totale perdita dei dati.

> *È molto difficile affermare che un virus sia totalmente innocuo, perché l'infezione può spesso portare a conseguenze imprevedibili e non volute nemmeno dal programmatore.*

II. Difendersi dai virus

Difendersi dai virus dei file

- Procuratevi un antivirus recente e aggiornatelo settimanalmente attraverso Internet, per aggiungere le informazioni sui virus recenti.
- Eseguite sistematicamente copie di riserva dei vostri dati (backup).
- Non installate sul computer qualsiasi tipo di software che vi viene prestato: serve anche per evitare di sovraccaricare inutilmente il sistema.
- Controllate con l'antivirus i documenti e i programmi che vi vengono dati.
- Non lasciate dischi floppy inseriti all'accensione del computer: serve per proteggervi dai boot virus.
- Acquistate software originale; anche se bisogna dire che qualche volta è capitato che distributori famosi abbiano messo in commercio software infetto.

Difendersi dai virus su Internet

- Utilizzate un antivirus che sia in grado di filtrare gli allegati di posta elettronica e controllare le pagine Web.
- Aggiornatelo settimanalmente attraverso Internet.
- Scaricate il software solo da banche dati affidabili (es. Simtel, Tucows).
- Evitate i siti pornografici e i siti pirati.
- Cancellate, prima di aprirle, le e-mail che hanno titoli strani (es. “I Love You”) e che provengono da sconosciuti.
- Cancellate, prima di aprirle, le e-mail che contengono allegati con nomi strani (es. “patch.exe”) e che non avete richiesto, anche se provengono da amici.
- Non fate circolare le “catene di S. Antonio”.
- Controllate con l'antivirus gli allegati di posta elettronica e il materiale che prelevate da Internet.

III. Approfondimenti

Introduzione

In questo capitolo riporto alcuni approfondimenti sui virus che sono rivolti esclusivamente ad utenti esperti. Consiglio pertanto di tralasciare le parti che non riuscirete a comprendere.

Algoritmi utilizzati dai virus

- **TSR capability** (Terminate and Stay Resident): capacità del virus di rimanere residente nella memoria RAM anche dopo che il programma infetto è terminato.
- Uso di **algoritmi Stealth** (di invisibilità) per nascondere le proprie tracce all'occhio vigile degli antivirus. I virus che utilizzano questa tecnica, spesso curano temporaneamente i file infetti per nascondere l'infezione.
- **Self encryption** e **polimorfismo**: capacità di crittografare o variare il proprio codice per non farsi identificare.
- Utilizzo di **tecniche non standard** come ad esempio creare una propria copia nella ROM del BIOS.

La **RAM** (*Random Access Memory – memoria ad accesso casuale*) è la memoria utilizzata dal computer per memorizzare temporaneamente i risultati delle variabili e delle operazioni svolte. Si tratta di una memoria di appoggio di tipo volatile, ossia viene cancellata quando il computer viene spento.

Il **BIOS** (*Basic Input Output System – sistema per gestire gli ingressi e le uscite elementari*) è un programma contenuto all'interno della scheda madre del computer (ossia la scheda dove vengono montati tutti i componenti) che gestisce alcune funzioni elementari dei componenti elettronici. È memorizzato in una memoria di tipo **ROM** (*Read Only Memory – memoria a sola lettura*). Viene aggiornato raramente, quando ci sono problemi relativi al computer imputabili ad una cattiva programmazione di fabbrica. Tale operazione viene svolta esclusivamente da tecnici qualificati, utilizzando un apposito software.

È un arduo compito per un virus insediarsi nel BIOS, poiché in commercio esistono diversi tipi di ROM che si programmano in modo differente, a seconda del costruttore e del modello della scheda madre. Attualmente esistono alcuni virus (Win.CIH del 1999, Magistr del 2001) che si diffondono con le tecniche standard è che in più sono in grado di alterare il contenuto del BIOS, in modo tale da rendere il computer non più avviabile.

Ma non ci sono solo i virus

- **Cavallo di Troia (Trojan horse)**: si tratta di un programma, generalmente distribuito su Internet, che finge di svolgere alcune funzioni utili o interessanti, ma che in realtà distrugge parzialmente o totalmente i dati o causa malfunzionamenti.
- **Verme (worm)**: è un programma distruttivo, in grado di moltiplicarsi, che però non si attacca ad altri programmi (quindi non richiede un ospite). Talvolta fa assumere alla propria copia il nome di un programma comunemente utilizzato dall'utente o dal sistema operativo (es. install, setup, start), in modo da venire mandato in esecuzione per sbaglio.
- **Programma per costruire i virus (virus construction set)**.
- **Finto virus o scherzo**: è un programma assolutamente innocuo che però visualizza dei messaggi catastrofici del tipo: "sto distruggendo il contenuto del tuo computer".
- **Falso allarme (hoax o "bufala")**: si tratta di messaggio del tipo "catena di S. Antonio", quasi sempre spedito per posta elettronica, che dà informazioni su come individuare ed eliminare un nuovo tipo di virus. Ignoratelo nella maniera più assoluta e non seguite i consigli che vi vengono dati, altrimenti rischiate di andarvi a cacciare in situazioni poco piacevoli.

I cavalli di Troia devono il loro nome al famoso espediente escogitato da Ulisse per conquistare la città del re Priamo. Proprio come il cavallo di legno, offerto in dono agli abitanti di Troia, celava al suo interno soldati armati, i programmi di questa categoria sembrano all'apparenza software legittimi, mentre invece svolgono funzioni tutt'altro che utili.

> *Possiamo considerare cavalli di troia anche quei programmi (spesso presenti sui siti pornografici) che, con la scusa di offrirci servizi Internet esclusivi e particolari, si collegano a computer remoti con telefonata intercontinentale.*

IV. La sicurezza informatica

Attacco informatico

Per *attacco informatico* si intende un tentativo d'intrusione nel nostro computer da parte di uno sconosciuto, mentre siamo connessi ad Internet. Il rischio maggiore si ha quando "chattiamo", poiché stiamo interagendo direttamente con una persona che non conosciamo e che potrebbe avere cattive intenzioni. Il malintenzionato potrebbe utilizzare un programma d'intrusione per entrare nel nostro computer e prelevare o cancellare dei documenti. Per difenderci si può utilizzare un particolare tipo di programma, denominato ***firewall*** (*lett. Tagliafuoco*), che analizza la trasmissione delle informazioni e blocca i tentativi d'intrusione.

Un discorso a parte va fatto per le aziende o gli enti che sono collegati permanentemente ad Internet. Per loro il rischio è esteso nell'arco dell'intera giornata; per difendersi utilizzano dei dispositivi elettronici, chiamati anch'essi firewall (*firewall hardware* per essere precisi), che analizzano il transito delle informazioni verso la rete Internet. Si tratta di dispositivi molto più efficaci dei *firewall software* ed estremamente costosi.

Chi ha la volontà, i mezzi e le capacità per attuare un attacco informatico consistente, non va certo a prendere di mira un privato, perché in genere l'obiettivo è quello di fare un atto dimostrativo che susciti fermento nell'opinione pubblica. Possiamo quindi stare tranquilli: per noi il firewall software (che si trova anche gratuitamente su Internet) è più che sufficiente; inoltre consiglio di montarlo solo nel caso in cui abbiate l'abitudine di passare molte ore nelle chat.

La privacy

Si parla sempre più spesso di privacy su Internet, perché sempre più frequentemente vengono raccolte informazioni a nostra insaputa: i siti contano gli accessi e calcolano le fasce orarie più gettonate, i motori di ricerca fanno statistiche sugli argomenti che le persone richiedono maggiormente, le aziende che offrono l'abbonamento gratuito ad Internet controllano i siti a cui ci colleghiamo e tracciano il nostro profilo di consumatore, per mandarci un tipo di pubblicità mirata.

Recentemente si è scoperto che alcuni programmi approfittano del momento in cui siamo connessi ad Internet per mandare al costruttore informazioni sul nostro computer. In pratica vogliono sapere che tipo di software e di hardware abbiamo installato sul nostro computer e verificano anche se il prodotto è stato regolarmente registrato. Ovviamente le informazioni, così rubate, non sono valide ai fini di accertamenti fiscali ma vengono solo utilizzare a scopo statistico. A causa di questi comportamenti, sono sorte negli Stati Uniti diverse cause tra le associazioni dei consumatori e le più grandi case produttrici di software.

Attraverso un firewall ci si può accorgere quando un programma tenta di inviare delle informazioni attraverso Internet ed eventualmente bloccarlo, anche se non ci è dato di sapere quali informazioni stia inviando. Ovviamente sia il programma di navigazione che il programma di posta trasmettono delle informazioni quando li utilizziamo: se li blocchiamo non possiamo più spedire le e-mail o visitare i siti Internet. Consiglio quindi la massima prudenza nell'uso di questi strumenti.

La crittografia

Cifrare un documento (o più in generale dei dati) significa renderlo illeggibile con lo scopo di impedire a malintenzionati di venire a conoscenza del contenuto. Soltanto il mittente e il destinatario conoscono la chiave per potere decifrare il messaggio. Queste tecniche venivano già utilizzate nell'antichità, quando due regnanti volevano scambiarsi delle lettere e impedire che durante il tragitto qualcuno si impossessasse del contenuto del messaggio.

Su Internet si utilizzano trasmissioni cifrare quando si trasmettono dati importanti come ad esempio il numero di carta di credito durante gli *acquisti on-line*. Mentre il programma di navigazione è in grado di gestire trasmissioni cifrate senza dovere installare moduli aggiuntivi, la stessa cosa non vale per il programma di posta elettronica: il supporto per la crittografia è spesso mancante o insufficiente. Esistono in commercio programmi per cifrare i messaggi di posta elettronica, PGP (Pretty Good Privacy) ne è un esempio: lo potete scaricare gratuitamente per uso non commerciale dal sito www.pgpi.org.

Il consiglio che posso dare è il seguente: per quel che riguarda gli acquisti on-line, fateli solo da aziende che ritenete affidabili e accertatevi che la trasmissione sia cifrata (deve apparire il simbolo di un lucchetto chiuso, all'interno della finestra del vostro programma di navigazione). Evitate assolutamente di trasmettere informazioni confidenziali per posta elettronica, se proprio lo dovete fare affidatevi a dei programmi di crittografia oppure utilizzate il fax.

Come funziona la crittografia

La differenza tra i messaggi scritti cifrati con le tecniche standard e gli omologhi di posta elettronica consiste nel fatto che, in quest'ultimo caso, la chiave viaggia assieme ai messaggi, rendendo il sistema effettivamente meno sicuro. Per rendere sicura la trasmissione è stato inventato un sistema che funziona con due chiavi: la chiave pubblica e la chiave privata. La chiave pubblica serve soltanto per codificare il messaggio e viene distribuita a tutte le persone che ne fanno richiesta; quella privata, invece, serve per decodificare il messaggio e viene conservata gelosamente dal proprietario. Le due chiavi funzionano in coppia, nel senso che la chiave privata può decodificare solo i messaggi prodotti con l'omologa chiave pubblica. Se Massimo vuole mandare un messaggio ad Andrea, deve cifrare il messaggio con la chiave pubblica di Andrea e poi spedirglielo. Dal momento che il messaggio può essere decodificato solo dalla chiave privata di Andrea e dal momento che soltanto quest'ultimo ne è in possesso, allora la trasmissione può definirsi sicura. Naturalmente i programmi di crittografia svolgono queste funzioni in maniera automatizzata, l'unica cosa che è richiesta la prima volta che si usa il programma è la creazione delle due chiavi.

La firma digitale

La firma digitale è un codice speciale, rilasciato da un ente accreditato, che apposto ai messaggi ne attesta l'autenticità del mittente. Il sistema funziona sempre con due chiavi (una pubblica e una privata) e sfrutta un sistema analogo di codifica a quello visto in precedenza, con una differenza: questa volta la chiave pubblica è quella che serve per decifrare e la chiave privata è quella che serve per cifrare. Se il Comune di Spilamberto vuole firmare digitalmente i propri messaggi di posta elettronica si deve rivolgere ad un ente di certificazione che gli deve rilasciare le due chiavi. Dal momento che soltanto la chiave pubblica del Comune di Spilamberto è in grado di aprire i messaggi firmati con l'omologa chiave privata (in possesso solo al Comune) e dal momento che le chiavi sono state rilasciate da un ente accreditato che ha anche la funzione di vigilare, quando Luca riceverà un messaggio dal Comune, potrà essere certo della sua autenticità e provenienza.

Indirizzi utili

Computer Associates – eTrust Antivirus – www.cai.com
Frisk Software International – F-Prot Antivirus – www.complex.is
Trend Micro – PC-cillin (antivirus) – www.trendmicro.it
Symantec – Norton Antivirus – www.symantec.it
McAfee – VirusScan (antivirus) – www.mcafee.com
PGPi – PGP (Pretty Good Privacy) – www.pgpi.org
Internet Security Systems – BlackICE PC Protection (personal firewall) – www.iss.net
Zone Labs – Zone Alarm (personal firewall) – www.zonelabs.com