1.6.2 MALWARE

1.6.2.1

Definire il termine "malware". Identificare diversi tipi di malware, quali virus, worm, Trojan, spyware

Quando, non moltissimi anni fa, i giornali e la televisione cominciarono a parlare di virus informatici, qualcuno pensò che si trattasse di nuove malattie che potevano contagiare l'organismo umano. Oggi, la situazione è un po' migliorata, e tutti (o quasi) sanno che un virus informatico consiste in un piccolo programma creato per provocare danni ai computer, per diffondersi nel computer stesso e da un elaboratore all'altro.

Intanto, con il passare degli anni, sono comparsi altri tipi di *software malevoli* per cui oggi si preferisce parlare di malware (pr. *mal-uèr*, da "MALicious softWARE", sign. "programma malvagio") per indicare genericamente qualsiasi tipo di software in grado di sottrarre informazioni creare danni: non solo virus, ma anche worm, trojan, spyware, ecc.

I worm (pr. *uòrm*, sign. "verme") si propagano principalmente attraverso la posta elettronica. Quando un computer o un altro tipo di dispositivo elettronico è contagiato da un *worm* comincia, infatti, a inviare automaticamente dei messaggi di posta elettronica a tutti gli indirizzi presenti nella rubrica, sfruttando i momenti nei quali un qualsiasi utente del computer infetto si collega a Internet e senza che la persona stessa se ne accorga. A ognuno di questi messaggi è allegato una copia dello stesso *worm:* la persona che riceve quel messaggio, confortato dal fatto che conosce il mittente, è spesso portata ad aprire l'allegato e contagia in quel modo il proprio computer. Attraverso questa continua moltiplicazione il virus occupa sempre maggiore spazio nella memoria del computer, rallentandone notevolmente le prestazioni.

I trojan (pr. *tròjen*, accettata anche *tròian*) o cavalli di Troia, che prendono questo nome proprio perché la loro strategia assomiglia a quella utilizzata da Ulisse per penetrare con i suoi compagni nella città di Troia, nascosti all'interno di un enorme cavallo di legno. I *trojan*, infatti, penetrano nel computer nascosti in altri programmi e cominciano a raccogliere informazioni riservate sulla persona che utilizza quel computer (nome utente, password, altri codici come ad esempio quelli delle carte di credito utilizzate per acquisti via Internet) per poi inviare queste informazioni a dei *cracker* (pr. *crècher*, sono i principali creatori dei virus) mentre il computer è collegato a Internet. Alcuni *trojan* permettono al *cracker* di controllare via Internet il computer su cui è installato il virus, ovviamente sempre e solo quando questo computer è collegato in rete. A quel punto il malintenzionato può visionare l'intero contenuto del disco, copiarlo modificarlo o cancellarlo a suo piacimento, in qualche caso persino controllare quanto succede nella casa del proprietario del computer se a questo sono collegati e accesi un microfono e/o una webcam.

Gli spyware (pr. *spàiuer*, da "SPY softWARE", sign. "programma per spiare") sono un tipo di software che, soprattutto durante la navigazione su Internet, trasmettono a nostra insaputa una serie di dati che ci riguardano (ad esempio i siti visitati) a dei computer esterni, che elaborano tali dati e provvedono a inviarci messaggi pubblicitari in base alle nostre abitudini e preferenze. Se, ad esempio, visitiamo con una certa

frequenza siti riguardanti il mondo delle automobili, quando ci collegheremo ad altri siti vedremo apparire nelle loro pagine delle pubblicità riguardanti la vendita di automobili o di prodotti ad esse correlati. A volte, il termine *spyware* viene utilizzato impropriamente anche per indicare versioni "ibride" di malware che possono provocare danni molto gravi, come i worm e i trojan che installano nei computer dei malcapitati un programma (detto keylogger, pr. *kì-lóggher*) che memorizza tutti i caratteri battuti sulla tastiera (documenti, e-mail, password, ecc.) per poi trasmetterli, mentre è in atto un collegamento a Internet, al malintenzionato che ha inviato questo tipo di malware.

I danni provocati dal malware possono essere di varia natura: furto e trasmissione all'esterno di dati custoditi nel dispositivo elettronico, comparsa di scritte o immagini indesiderate, messaggi d'errore, rallentamento del dispositivo, impossibilità di utilizzare alcune applicazioni e altro ancora. Spesso, senza un apposito programma antivirus, è difficile capire se il danno è causato da un malware o da un problema dovuto al malfunzionamento del software o dell'hardware.

In alcuni casi, per poter riutilizzare il dispositivo è necessario cancellare (per la precisione *formattare*) l'intero contenuto della memoria interna e ricaricare tutte le applicazioni e i documenti ricopiandoli sul proprio computer da chiavi USB, dischi fissi esterni, altri dispositivi di memoria, e questo rappresenta un problema molto serio, specie per chi non ha l'abitudine di conservare copie aggiornate di quanto ha scritto o memorizzato sul proprio computer.

1.6.2.2 Sapere come un malware può infettare un computer o un dispositivo

Proprio come i virus biologici – che infettano l'organismo penetrando in esso - così i virus informatici e i malware in generale, possono infettare un computer soltanto arrivando dall'esterno. Per comprendere quali possono essere le modalità di trasmissione dobbiamo ricordare che un computer o un dispositivo è connesso a periferiche di input e di output, cioè a canali d'ingresso e di uscita.

I canali di comunicazione con l'esterno, in particolare quelli d'entrata (input), sono le vie attraverso le quali un malware può penetrare nel computer o nel dispositivo. Essi sono principalmente:

- la connessione a una rete, a cominciare dalla più grande tra esse, vale a dire Internet;
- i messaggi di posta elettronica;
- le unità esterne di memoria (penne USB, CD e DVD).

La penna USB è molto usata per trasferire file di testo o altri documenti da un computer all'altro: pensiamo ai comuni file generati con *Word* o *Excel*. Ebbene, se trasferiamo frequentemente file da un computer all'altro, aumentano le probabilità che un malware proveniente da un computer infetto contamini il nostro o un altro computer. Anche CD e DVD possono produrre infezioni: file infetti masterizzati e poi copiati da un computer all'altro conducono allo stesso risultato, così come software di provenienza incerta. Lo stesso discorso vale per altre unità esterne di memoria (ad es. dischi fissi esterni); anche documenti registrati da molto tempo, se infetti, possono provocare la contaminazione.

Rischi d'infezione maggiori provengono dall'utilizzo di Internet e dalle reti in generale, per la grande quantità d'informazioni che vengono trasferite con grande velocità. Navigando da un sito all'altro, scarichiamo

infatti nel nostro computer parecchi megabyte d'informazioni e, più aumenta la mole di dati, maggiori sono i rischi.

Attualmente, però, la più diffusa fonte d'infezione da malware è la posta elettronica, in particolare gli allegati. Spesso, a nostra insaputa, i malware fanno partire messaggi infetti a tutti i nominativi contenuti nella nostra *Rubrica* dell'applicazione che utilizziamo per la posta elettronica (ad es. *Windows Mail* o *Outlook*). Una prima precauzione che possiamo prendere è quella di non aprire messaggi di provenienza sconosciuta o senza *Oggetto*, in particolare se contengono allegati con estensioni *exe com bat vbs scr pif* e di non cliccare su eventuali collegamenti (*link*) presenti in questi messaggi, ma questo serve solo a limitare i danni. Una soluzione può essere quella di controllare la posta direttamente sul sito del provider col quale abbiamo un account ed eliminare (anche dal *Cestino*) i messaggi sospetti, ma, senza un buon antivirus costantemente aggiornato, la probabilità che il nostro PC possa essere attaccato da un malware resta molto elevata.

1.6.2.3

Usare un software antivirus per eseguire una scansione in un computer

Per saperne di più...

– su antivirus e firewall, acquisisci l'immagine del QR Code con il tuo smartphone o tablet.

Un'applicazione antivirus rappresenta, dunque, una necessità per ogni computer. Sistemi operativi recenti come *Windows 8* integrano già un antivirus e ne esistono anche per altri dispositivi come tablet e smartphone.

In genere, all'installazione dell'antivirus, le impostazioni predefinite configurano già l'applicazione per gestire automaticamente:

- la scansione (vale a dire l'analisi) iniziale dei record di avvio del computer e di alcuni file a ogni accensione;
- la scansione di un file quando esso viene aperto con un'applicazione;
- la scansione di supporti rimovibili (penne USB, schede di memoria, CD, DVD, ecc.);
- la protezione del computer durante l'esplorazione di siti Internet;
- la scansione dei messaggi di posta elettronica e degli eventuali allegati;
- l'aggiornamento automatico dell'applicazione a intervalli regolari mentre il computer è connesso a Internet.

Un antivirus ben configurato e costantemente aggiornato, rende improbabile che un malware possa introdursi nel computer; è comunque consigliabile avviare di tanto in tanto manualmente la scansione del computer, oppure di file o cartelle sospette.

Basterà utilizzare il comando *Scansione* (o *Scan,* o *Scan for viruses* o simili) dopo aver selezionato il disco, la cartella o il file che vogliamo controllare. Solitamente, una volta installato nel computer, l'antivirus può essere avviato anche dal menu contestuale che appare cliccando (su un disco, una cartella o un file) con il tasto destro e poi scegliendo la voce – diversa a seconda dell'antivirus – *Scan, Avvia scansione* o simili.

Se sono presenti malware, l'antivirus ne indicherà il tipo e suggerirà la procedura da eseguire: se disinfettare, mettere in quarantena oppure eliminare il file. Queste opzioni dipendono dal tipo di malware:

- *Disinfetta:* l'antivirus è in grado di eliminare il malware dal file infetto e restituirci il file com'era prima dell'infezione.
- *Metti in quarantena:* l'antivirus non è in grado di disinfettare il file contagiato, lo posiziona quindi in una cartella protetta in attesa di scaricare dalla casa produttrice dell'antivirus un aggiornamento che permetta di eliminare quel tipo di malware.

- *Elimina:* il programma non è in grado di svolgere le prime due operazioni e quindi l'unica soluzione è l'eliminazione del file.

Quest'ultima opzione riguarda spesso i CD e i DVD, sui quali il programma non può intervenire giacché, una volta inciso, il dischetto a lettura ottica non è modificabile. Non essendo possibile eliminare il file da un CD o DVD, essi sono inservibili (a meno di voler infettare il computer).