Uso del computer e gestione dei file (virus)

Modulo 2

Utilità (dal Syllabus)

- *Compressione di file*
  - …
  - Utilizzare un'applicazione antivirus per controllare unità, cartelle e file specificati.
  - Comprendere per quale motivo è necessario aggiornare regolarmente il software antivirus.

Virus *(da Wikipedia)*

- *Nell'ambito dell'informatica un virus è un software, appartenente alla categoria dei malware, che è in grado, una volta eseguito, di infettare dei file in modo da riprodursi facendo copie di sé stesso, generalmente senza farsi rilevare dall'utente.*
- *I virus possono essere o non essere direttamente dannosi per il sistema operativo che li ospita, ma anche nel caso migliore comportano un certo spreco di risorse in termini di RAM, CPU e spazio sul disco fisso.*
- *Come regola generale si assume che un virus possa **danneggiare** direttamente solo il **software** della macchina che lo ospita, anche se esso può indirettamente provocare danni anche all'hardware, ad esempio causando il surriscaldamento della CPU mediante overclocking, oppure fermando la ventola di*

Malware

- *Nell'uso comune il termine virus viene frequentemente ed impropriamente usato come sinonimo di **malware**, indicando quindi di volta in volta anche categorie di "infestanti" diverse, come ad esempio worm, trojan o dialer.*
- *Si definisce **malware** un qualsiasi software creato con il solo scopo di causare danni più o meno gravi al computer su cui viene eseguito. Il termine deriva dalla contrazione delle parole inglesi **malicious** e **software** e ha dunque il significato letterale di "**programma malvagio**"; in italiano è detto anche codice maligno.*

Tipi di Malware

- **Worm** (letteralmente "verme") è una particolare categoria di malware in grado di autoreplicarsi. È simile ad un virus, ma a differenza di questo non necessita di legarsi ad altri eseguibili per diffondersi.
- **Trojan** o trojan horse (dall'inglese per Cavallo di Troia), è un tipo di malware. Deve il suo nome al fatto che le sue funzionalità sono nascoste all'interno di un programma apparentemente utile; è dunque l'utente stesso che installando ed eseguendo un certo programma, inconsapevolmente, installa ed esegue anche il codice trojan nascosto.
- **Dialer** è un programma per computer che crea una connessione ad Internet, a un'altra rete di calcolatori o semplicemente a un altro computer tramite la comune linea telefonica.

Cos'è un virus

- Un virus è composto da un insieme di istruzioni, come qualsiasi altro programma per computer.
- Caratteristica principale di un virus è quella di riprodursi e quindi diffondersi nel computer ogni volta che viene aperto il file infetto.
- Tuttavia, un virus di per sé non è un programma eseguibile, così come un virus biologico non è di per sé una forma di vita. Un virus, per essere attivato, deve infettare un programma ospite.
- La tecnica solitamente usata dai virus è quella di infettare i file eseguibili: il virus inserisce una copia di sé stesso nel file eseguibile che deve infettare, pone tra le prime istruzioni di tale eseguibile un'istruzione di salto alla prima linea della sua copia ed alla fine di essa mette un altro salto all'inizio dell'esecuzione del programma.
- In questo modo quando un utente lancia un programma infettato viene dapprima impercettibilmente eseguito il virus, e poi il programma.

Cosa può fare un virus

- Attaccare i file. I virus possono eliminare o corrompere i file esistenti e anche riempire il computer di file inutili.
- Attaccare la posta elettronica. I virus possono leggere la vostra posta elettronica, inviare messaggi da chiunque a tutti (persone che conoscete e anche sconosciute) e persino trasformare il vostro computer in un ufficio postale, consentendo all'autore del virus di inviare posta attraverso il vostro computer.
- Danneggiare l'hardware. I virus possono danneggiare l'hardware e qualsiasi periferica collegata.
- Rubare i dati personali. I virus possono rubare i vostri dati personali e informazioni preziose (tra cui password e numeri di carta di credito).
- Creare molti fastidi. I virus possono riavviare il sistema in continuazione, impedirne l'avvio, visualizzare messaggi volgari e fastidiosi e quant'altro.

Modalità di diffusione dei virus

- Prima della diffusione su larga scala delle connessioni ad Internet, il mezzo prevalente di diffusione dei virus da una macchina ad un'altra era lo scambio di floppy disk contenenti file infetti. Il veicolo preferenziale di infezione è invece oggi rappresentato dalle comunicazioni e-mail e dalle reti di peer to peer.
- Nei sistemi informatici Windows è di consuetudine usare il registro di sistema per inserire in chiavi opportune dei nuovi programmi creati ad hoc dal programmatore di virus che partono automaticamente all'avvio. Uno dei punti deboli del sistema Windows è proprio il suo registro di configurazione. Esistono vari programmi per tenere d'occhio le chiavi pericolose del registro di Windows.

Antivirus

- Un antivirus è un software atto a rilevare ed eliminare virus informatici o altri programmi dannosi (malware.
- Tecniche usate dagli antivirus:
  - **Monitoraggio**: prevenire un'infezione mediante il controllo di attività sospette (ad esempio, la richiesta di formattazione di un disco oppure l'accesso a zone privilegiate di memoria).
  - **Scanner**: confronto tra le firme memorizzate in un **database interno**, con quelle, eventualmente, contenute nei file infetti (importantissimo l'aggiornamento del database dei virus);
  - **Verifica dell'integrità**: calcolano l'hash dei file da confrontare successivamente coi nuovi valori risultanti da un nuovo calcolo per verificare che i file non abbiano subito modifiche nel frattempo.

Per evitare virus è sufficiente installare un software antivirus?

- No: un software antivirus è un buon inizio, ma per molti motivi non è sufficiente limitarsi ad averlo installato.
- Esso deve essere attivo, aggiornato con l'ultimo motore di scansione e con le definizioni più recenti, registrato in modo da ricevere gli aggiornamenti e configurato in modo corretto.