Corso Integrato di Statistica Informatica e Analisi dei Dati Sperimentali

Note A.A. 2009-10

C. Meneghini

1 Informatica (Modulo III)

1.1 Sicurezza del PC e delle informazioni

Il personal computer (PC) é sempre di piú uno strumento indispensabile non solo per il lavoro ma anche per la vita sociale. Quando si utilizza un PC bisogna tenere ben presente il fatto che, se da un lato i dati in formato elettronico hanno caratteristica (assai vantaggiosa) di essere disponibili in gran quantitá, in modo rapido e di poter essere velocemente diffusi e pubblicati. D'altronde essi possono essere anche rapidamente alterati, distrutti e definitivamente persi. Su un disco rigido sono spesso registrate informazioni importanti, raccolte in anni di attivitá: la perdita di questi dati puó avere effetti irrimediabili non solo in ambito professionale. Inoltre i dati dati raccolti sul proprio PC contengono spesso informazioni strettamente personali che, se diffuse, potrebbero avere effetti spiacevoli.

La migliore difesa contro la perdita (o il furto di dati), accidentale o dolosa che sia, consiste nel tenersi adeguatamente informati sulle modalitá di protezione e recupero dei dati contenuti nel proprio PC. In particolare, per prevenire azioni dolose, é bene tenersi informati sui metodi utilizzati per danneggiare o carpire informazioni dal proprio PC, quindi sulle caratteristiche dei virus informatici, sulle tecniche utilizzate per il contagio e diffusione dei virus, sulle tecniche di difesa e prevenzione.

Proteggere il proprio PC (o un sistema informatico in genere) significa prevenire eventi accidentali o dolosi che possano alterare o distruggere le informazioni registrate in formato elettronico nelle unitá di memoria di massa (dischi rigidi, supporti USB, etc...). In particolare proteggere significa garantire:

- la riservatezza delle informazioni registrate, queste devono essere accessibili alle sole persone autorizzate;
- l'integritá dei dati e delle informazioni contenute: solo le persone autorizzate devono poter modificare o alterare le informazioni contenute nel sistema;
- la disponibilitá delle risorse e delle informazioni contenute.

e, in caso di danno, si devono poter recuperare le informazioni e ripristinare le funzionalitá della macchina.

Il proprio PC contiene dati di interesse personale anche assai importanti sia dal punto di vista soggettivo (es.: la copia della tesi di laurea, indirizzari di amici, documenti, foto) sia oggettivo (es. numeri di conti correnti, numeri di carte di credito, password, etc...) quindi perdere questi dati puó essere non solo spiacevole, ma anche avere conseguenze gravi, dal momento che alcune di queste informazioni potrebbero essere usate da terzi per scopi illeciti.

Quando poi si utilizza un PC in ambito professionale si puó avere a che fare con con dati che riguardano terze persone e con una classe particolare di dati, quelli che riguardano aspetti personali e sensibili degli individui: i *dati personali*. Il trattamento dei dati personali in formato elettronico é una materia complessa e delicata. Queste note sono scritte per studenti di Biologia nella cui vita professionale si potrebbero trovare ad utilizzare e maneggiare dati personali estremamente sensibili se, ad esempio, impiegati in laboratori di analisi. E' bene quindi informarsi sulla normativa e sui rischi che si corrono nel trattare con leggerezza dati sensibili.

In tutti i paesi esiste una normativa contenente disposizioni in campo di sicurezza informatica, atte a proteggere i dati di terze persone. In Italia esiste un insieme di *misure minime di sicurezza* obbligatorie per chi tratti dati in formato elettronico. Dal momento che non adottare le misure minime previste dalla normativa é punibile penalmente, queste devono essere conosciute e tenute in conto soprattutto da chi abbia accesso a dati personali di terze persone. In italia queste norme sono pubblicate sul sito del Garante della Privacy[1].

Attenzione, l'adozione delle *misure minime di sicurezza* puó prevenire un'azione penale, tuttavia é previsto che chiunque cagioni danno ad altri per effetto del trattamento dei dati personali sia perseguibile civilmente, sará quindi tenuto a dimostrare di aver adottato tutte le misure idonee ad evitare il danno. E' quindi evidente che, per chi utilizza i computer nella vita privata e/o professionale, é fondamentale conoscere e tenersi aggiornato sugli aspetti riguardanti la sicurezza e la protezione dei dati propri e, a maggior ragione, di terze persone.

I rischi di danneggiamento cui é esposto un PC possono essere di tipo fisico (hardware) o software. Nel primo caso i danni riguardano parti fisiche del PC (dischi, schede, supporti USB, etc...) che possono essere causati da semplice usura o da fenomeni fisici (es.: acqua, urti, cadute, shock elettrici, etc...). Danni di questo tipo sono generalmente accidentali, spesso non prevedibili. Per prevenire la perdita dei dati a causa di danni accidentali é bene effettuare backup frequenti dei dati e del software che si utilizza. Il rapido aumento di dimensioni dei dischi rigidi e della quantitá di informazioni che

[1] *www.garanteprivacy.it* o simile: considerate che a volte i siti WEB cambiano di indirizzo e quindi alcuni link forniti in queste note potrebbero risultare sbagliati

si raccolgono, rende l'uso di CD o DVD poco pratico per un backup frequente. Piú semplice é l'impiego di un secondo disco rigido interno (piú economico ma piú complicato da montare) o un disco rigido esterno (dotato, ad esempio di interfaccia USB) su cui salvare di volta in volta il proprio lavoro e i dati piú importanti. Per effettuare il backup esistono software specifici, ovvero si possono semplicemente copiare i dati importanti, i piú esperti possono preparare programmi e istruzioni ad hoc. Un'aspetto fondamentale da tenere a mente é che anche CD, DVD, dischi rigidi invecchiano e i dati possono risultare illegibili dopo alcuni anni: un buon CD/DVD ha una durata media di 5-10 anni.

I rischi di danneggiamento di tipo software sono di gran lunga piú probabili e frequenti. Danni di questo tipo possono derivare da cause accidentali, da errori umani (es.: per sbaglio si possono cancellare o sovrascrivere files e dati) o dei programmi utilizzati (es.: bugs, problemi di incompatibilità, etc...). Molto piú spesso sono dovuti a software specificamente creati per creare danni e disturbi, i cosiddetti **virus** o, piú in generale, **malware**. Conoscere il funzionamento dei malware é il primo passo per imparare ad evitarli. Vediamo di seguito un elenco dei tipi di malware piú diffusi, classificati in base al loro funzionamento.

1.2 Classificazione dei Malware

In effetti il termine VIRUS, coniato per i primi software dannosi all'inizio degli anni 80, si é rivelato decisamente restrittivo per classificare l'ampia verietá di programmi utilizzati per danneggiare, carpire informazioni o semplicemente disturbare gli utenti di un PC. Si é quindi coniato il termine piú generico di **MALWARE** da *MAL*icious-soft*WARE*) per indicare un programma (o un codice) atto a provocare danni al PC e/o alle informazioni in esso contenute, ovvero che consenta la diffusione di dati e informazioni personali contenute nel PC (numeri di carte di credito, password, indirizzi di posta, etc...), ovvero che consenta l'accesso nascosto e non autorizzato al PC e alle informazioni contenute, ovvero... .

Su Wikipedia, cosi come su molti altri siti dedicati al problema della sicurezza, si puó trovare un'ampio e dettagliato elenco dei malware conosciuti classificati in base al loro modo di funzionamento e al tipo di danno o intrusione praticato. Di seguito riportiamo un breve descrizione dei principali. Non é un elenco esaustivo: dal momento che la fantasia di chi crea un malware é brillante e attiva almeno quanto quella di chi deve pensare alle difese, sono continuamente creati e diffusi nuovi tipi malware e nuove strategie di attacco, cui fanno seguito programmi di difesa e metodi di prevenzione.

- **Virus**: Cosí chiamati per l'analogia con i virus biologici, i virus informatici sono parti di codice che si annidano all'interno di un programma ospite modificandone il codice. Questi codici contengono istruzioni che provocano la replicazione del virus all'interno di altri programmi, nel software di sistema e nella memoria del PC. Durante la replicazione i codici possono eventualmente mutare (virus mutanti) in modo da renderene piú difficile l'individuazione. Provocano effetti dannosi o azioni di disturbo. Le principali vie di trasmissione dei virus sono lo scambio di files da dispositivi USB (chiavette, dischi), via Mail o su reti P2P. La diffusione mediante dischetti puó considerarsi oramai obsoleta. *Effetti* tipici dei virus possono essere: visualizzare messaggi o effetti video non voluti, cancellare files o formattare unitá disco, cifrare il contenuto di un disco rigido rendendolo illeggibile, rendere instabile il comportamento del sistema, impedire l'avviamento del PC o di programmi, modificare i dati all'interno di documenti, inviare messaggi di posta elettronica in modo massiccio (spamming). A loro volta i virus si possono classificare in:

  -*virus delle macro*: usano come veicolo le macro di pacchetti wordprocessor o fogli elettronici. Modificano le impostazioni dei programmi di videoscrittura e dei fogli elettronici.

  -*virus di avvio*: infettano il boot-sector dell'hard disk, dove sono le prime istruzioni eseguite durante la procedura di accensione del PC (bootstrap). In questo modo vengono attivati prima dell'antivirus e sono quindi piú difficili da rimuovere.

  -*virus di eseguibili*: si trovano all'interno di programmi eseguibili e si attivano all'attivarsi del programma.

  -*virus polimorfi*: sono in grado di modificare il proprio codice in modo da rendersi irriconoscibili all'antivirus. Possono mutare meccanismi di azione e di disturbo producendo copie sempre diversi.

  -*Logic-* e *time-bombs* sono virus che si attivano in concomitanza di azioni specifiche (es. combinazioni di tasti) o ad una data prefissata.

- **Worms**: I Worms sono codici contenenti istruzioni dannose che non hanno bisogno di un programma ospite per propagarsi ma si annidano direttamente nei sistemi operativi modificandone il codice. I worms si diffondono soprattutto utilizzando vulnerabilitá dei sistemi operativi o ingannando gli utenti. Si diffondono tramite Internet sfruttando difetti (bugs) dei sistemi operativi o di programmi. L'utente ignaro é indotto ad attivare il worm mediante trucchi e inganni di vario tipo (social engineering) spesso navigando su pagine WEB poco sicure: tipicamente siti che offrono software piratato, offerte particolarmente vantaggiose e simili. Molto

spesso un worm é fatto per disturbare le comunicazioni via rete occupando la banda di comunicazione. Un worm puó contenere codici per danneggiare il sistema ospite, cancellare i files o diffondere a terzi informazioni sensibili. Un'azione tipica del worm é quella di aprire una connessione nascosta (backdoor) sul PC infetto per consentire ad altri di utilizzare il PC via rete e prenderne il controllo. Si parla di Zombie computer: un PC la cui sicurezza é stata compromessa e si trova sotto il controllo di altri utenti. I worms Sobig e Mydoom sono tipici esempi di questo tipo.

- *e-mail worms*: si propagano attraverso la posta elettronica: il worm si installa nel sistema e si replica inviandosi a liste di corrispondenti utilizzando e-mail fasulle in cui il mittente é spesso mascherato in modo da non poter risalire facilmente all'origine dell'infezione.

-*Instant messaging worms*: si diffonde usando i messaggi istantanei (es.: windows messenger) fornendo link a siti infetti: collegandosi si attiva il download del worm all'insaputa dell'utente.

-*IRC worms*: usano i canali delle chat come bersaglio e metodo di infezione.

-*File sharing network worms*: si installano nelle directories condivise sulle reti P2P con nomi innocui e vengono scaricati e attivati dagli utenti.

-*Internet Worms*: usano protocolli di basso livello (TCP/IP) per propagarsi. Spesso utilizzando vulnerabilitá specifiche dei sistemi operativi.

- **Trojan horses**: (Cavalli di Troia) sono programmi con scopi illeciti che si nascondono all'interno di programmi apparentemente innocui. Non possiedono, generalmente, funzioni di autoreplicazione. Si propagano utilizzando la messagistica istantanea, usando i canali delle chat (IRC - Internet Relay Chat), gli allegati, i file condivisi (file sharing, P2P), possibili difetti dei browsers e dei client di posta elettronica. Esistono diversi tipi di Trojans, tra questi citiamo: *Remote Access Trojans* (consentono l'accesso al PC infetto in modo remoto), *Data Sending Trojans* (inviano dati a terzi in modo subdolo), *Destructive Trojans* (distruggono dati e informazioni), *Security software disabler Trojans* (disabilitano software di protezione quali firewall e antivirus), *Denial-of-service attack (DoS) Trojans* (impediscono l'avvio di servizi sul PC o server infetto), *DNS Trojans* (modificano i files dei Domain Name Server). Tra gli effetti principali di un trojan horse citiamo: cancellare dati, criptare files (es. a scopo di ricatto), danneggiare files, mandare e ricevere files in modo subdolo, registrare screenshots dell'attivitá dell'utente, registrare informazioni di login, registrare dati bancari, installare di backdoors, raccogliere indirizzari a fini di spamming, permettere l'accesso remoto ad altri (RAT-remote administration tool), favorire la diffusione di virus e malvare (vettore o untore) disattivando firewall e antivirus, creare network di computer zombie per spamming e attivitá illecite (es.: DoS attack)

- **Backdoor**: Programmi che aprono canali di comunicazione nascosti per consentire l'accesso al PC in modo remoto per scopi fraudolenti (acquisizione di informazioni, controllo del PC, etc...)

- **Spyware**: Sono programmi che utilizzati per collezionare informazioni (spiare) sul sistema infetto e trasmetterle a terzi in modo subdolo.

- **Dialer**: Sono oramai quasi obsoleti (almeno per i PC, ne esistono per pocket PC): dirottano le connessioni dei modem classici su numeri che forniscono servizi ad alto costo.

- **Hijacker**: Si occupano di dirottare la navigazione verso pagine web indesiderate (contenuto illecito, pubblicitario o pornografico).

- **Rootkit**: sono composti da driver modificati o copie modificate di normali programmi inseriti nel sistema. Hanno la funzione di mascherare sia all'utente che a programmi tipo antivirus la presenza di particolari file o impostazioni del sistema (es. nascondere le estensioni dei files, impedire la configurazione di antivirus, etc...). Possono essere utilizzati per nascondere o mascherare altro software dannoso.

- **Rabbit**: Sono programmi che esauriscono le risorse del sistema creando copie di se stessi molto rapidamente, fino ad occupare tutta la memoria rallentando praticamente le prestazioni del sistema.

- **Adware**: (advertising-supported software) installano sul computer contenuti pubblicitari non desiderati (es. finestre di pop-up e avvisi) spesso all'insaputa dell'utente.

- **Batch**: Sono i cosiddetti 'virus amatoriali': semplici files batch (istruzioni per DOS) che, se eseguiti, contengono istruzioni dannose.

- **Keylogger**: sono programmi in grado di registrare ció che un utente digita su una tastiera o con "copia e incolla" rendendo cosí possibile il furto di password o altre informazioni sensibili.

- **BHO** (Browser Helper Object). I plug-in sono programmi di piccole dimensioni progettati per espandere le funzionalitá di applicazioni come Browser e programmi per la posta elettronica. I Browser plug-in, in particolare, hanno caratteristiche rivolte

alla navigazione e ricerca su Internet. Un BHO non é di per se una minaccia fintanto che non si installa segretamente e non registra in modo subdolo le azioni dell'utente allo scopo di carpire informazioni e fornire dati a terze parti. Alcuni BHO cambiano l'home page del browser, e visualizzano finestre pop-up non richieste.

- **Spam**: non é di per se un malware ma un'azione di disturbo. Il termine spam indica comunicazioni non richieste e insistenti di prodotti anche illeciti e illegali. I messaggi Spam contengono spesso link a siti contenti materiale pornografico e/o offensivo e/o illegale etc... Il danno prodotto dallo spamming consiste principalmente nell'occupazione della capacitá dei server di posta, nel riempire le cartelle di posta degli utenti, nella perdita di tempo che comporta la localizzazione e rimozione di messaggi inutili e non richiesti. Molti provider hanno integrati filtri antispamming (es. gmail ha un'ottimo filtro antispamming)

- **Hoax**: Come lo spam gli Hoax (bufale/burle) non sono malware, tuttavia forniscono informazioni false o artefatte con avvisi di virus disastrosi, malattie, richieste di aiuto, casi umanitari, che quasi mai risultano vere. Un elenco aggiornato (italiano) si puó trovare su http://www.attivissimo.net/antibufala (come detto sopra le pagine WEB possono cambiare indirizzo, pertanto alcuni link potrebbero risultare inesistenti). Gli Hoax si diffondono principalmente via mail, chat, etc... Come regola é importante non diffondere in modo incontrollato avvisi, annunci, appelli e quant'altro. Per evitare di diffondere informazioni false e falsi allarmi, é bene fare un rapido controllo (on-line) per verificare le informazioni: spesso é sufficiente utilizzare un motore di ricerca inserendo alcune delle parole chiave contenute nel messaggio per ottenere un riscontro accurato.

- **Phishing**: anche questo non é propriamente un malware ma un'attivitá criminale, illegale a tutti gli effetti, tramite cui vengono acquisite informazioni sensibili (numeri di carte di credito, coordinate bancarie, password) mascherandosi da ente/societá/persona di fiducia. Il phishing avviene tramite e-mail o instant messaging. Spesso si forniscono link a siti web copia di siti accreditati (banche, enti, istituti). Quindi il consiglio è di non fornire per alcun motivo dati sensibili (password, numeri CC, coordinate bancarie) via web o e-mail.

- Altri tipi di malware sono i **Downloaders**: programmi che scaricano in modo subdolo applicazioni e contenuti per scopi illeciti. **Trackware**: (tracciatori) trasmettono informazioni sui siti visitati dall'utente.

Non essendoci limiti alla fantasia creativa del programmatore né alle possibilitá offerte dal mondo virtuale, possiamo lasciare aperta questa lista sottolineando come la classificazione data sia solo indicativa, molti malware (anche non particolarmente sofisticati) sfruttano una combinazione di tecniche di attacco, infezione e riproduzione mettendo insieme strategie proprie di diverse classi di malware.

1.3 Antivirus e Firewall

Una volta descritti per sommi capi le azioni e i danni che possono essere prodotti da un malware, vediamo come agire per difendersi. Antivirus a Firewall aggiornati sono, insieme ad un comportamento prudente, le armi migliori contro infiltrazioni di malware di vario genere. Antivirus a Firewall hanno entrambi lo scopo di proteggere il PC e i dati in esso contenuti ma hanno caratteristiche e scopi diversi: **gli antivirus** sono programmi che ricercano all'interno della memoria, dei files e dei programmi, la presenza di particolari sequenze di codice e istruzioni che caratterizzano ogni malware conosciuto: questi codici costituiscono la *firma* del Malware. Quando un nuovo malware viene scoperto sene pubblica la firma, i produttori di software antivirus includono le nuove firme in un file che viene aggiornato regolarmente: il file delle firme. Il successo di un antivirus risiede quindi nell'aggiornamento continuo del file delle firme (che di solito viene fatto in modo automatico ad intervalli fissati dall'utente in base alle sue necessitá) e nella scansione automatica di ogni file o programma attivato sul PC (resident shield). Esistono anche antivirus che si basano su algoritmi euristici per segnalare comportamenti sospetti ma, allo stato attuale, hanno uno scarso indice si successo e, il piú delle volte, segnalano come malevolo un comportamento del tutto lecito.

I moderni antivirus includono diversi moduli per assicurare la migliore protezione:

- il *file delle firme*, contenente le firme di tutti i virus scoperti, che deve essere regolarmente aggiornato;

- un modulo per l'aggiornamento automatico del file delle firme che puó essere opportunamente programmato a intervalli di poche ore, giorni o settimane. Ovviamente aggiornamenti poco frequenti aumentano il riscio di contagio. d'altronde aggiornamenti troppo frequenti possono rallentare il funzionamento del PC.

- Un modulo per effettuare la scansione dell'intero sistema (disco rigido, processi in memoria, dischi collegati etc...).

- Un modulo per la scansione di ogni file creato e/o modificato e/o trasferito da/sul disco.
- Un modulo per la scansione delle Mail e degli allegati in ingresso e in uscita.

Altri moduli, spesso presenti nei programmi antivirus, consentono lo scan delle pagine WEB e dei siti durante la navigazione oppure la protezione da spyware, adware e atri tipi di malware. Esistono diversi software antivirus, molti a pagamento, alcuni di shareware o freeware per uso personale. Spesso un antivirus freeware é piú che sufficiente per scopi di protezione personale, se associato ad un comportamento ragionevolmente prudente. Non esiste l'*antivirus migliore*, o l'*antivirus definitivo*, al contrario é bene tenersi informati sullo stato dell'arte e eventualmente esser pronti a sostituire il proprio antivirus con uno migliore basandosi sul consiglio di amici piú esperti, valutazioni pubblicati su siti dedicati, etc...

Il **Firewall** controlla gli accessi al sistema (PC) sia dall'esterno (Internet, supporti esterni) che dall'interno (programmi, processi, moduli) segnalando azioni *anomale* come ad esempio un programma che cerchi di attivare una connessione internet o attivare altri sottoprocessi o modificare impostazioni di sistema. Il Firewall controlla l'attivitá del sistema in base ad una serie di regole di comportamento e di interazione tra programmi. Queste regole sono definite dall'utente in un periodo di *apprendimento*: in pratica il firewall chiede all'utente come comportarsi di fronte a determinate richieste e situazioni. In questo modo si possono ammettere o vietare le diverse attivitá del PC in base a regole specifiche, che ovviamente possono essere anche modificate. Ogni volta che il firewall segnala un'azione per la quale non 'e prevista una regola l'utente é avvisato del comportamento anomalo, puó quindi decidere di conseguenza (es. definire una nuova regola). Se riconosce (o sospetta) un comportamento scorretto o pericoloso del sistema puó controllare e correre ai ripari prima della diffusione di un'eventuale infezione. E' importante sottolineare che un firewall non solo protegge il proprio PC ma puó anche evitare di diffondere le infezioni ad altri sistemi.

Una volta che il sistema sia stato infettato é assai improbabile che l'antivirus sia in grado di rimuovere il virus o il malware da solo. Infatti i codici piú sofisticati si annidano profondamente nel sistema disattivando in toto o in parte l'antivirus e il firewall, modificano le impostazioni del sistema per nascondersi e impedire azioni di ripristino e disinfestazione. Quindi la loro rimozione richiede una certa pratica e un lavoro a volte anche lungo. Cosa fare se il nostro PC risulta infetto? Purtroppo la disinfestazione da effettuare dipende dal tipo di infezione, dal sistema operativo, dagli strumenti a disposizione, quindi non é possibile dare una *ricetta* universalmente valida, d'altronde portare il PC da un esperto non é sempre l'idea migliore e non solo per motivi economici: riuscire a risolvere il problema ci permette di capire meglio il funzionamento del nostro PC e, magari, evitare in futuro di ricadere nelle stesse trappole.

Fermo restando che ogni infezione richiederá una cura ad hoc, supponiamo che l'antivirus abbia rilevato un malware. Innanzitutto mettiamo in quarantena il file (di solito é l'opzione di default dell'antivirus) quindi:

- dal momento che sospettimo un'infezione (a volte anche gli antivirus sbagliano, oppure, se siamo fortunati, rivelano un file infetto prima che l'infezione si sia diffusa) é utile eseguire l'analisi del PC utilizzandolo in modalitá provvisoria (in genere tenendo premuto il tasto F8 o F11 all'avvio il sistema offre diverse opzioni tra qui la possibilità di avvio in modalitá provvisoria). In modalitá provvisoria vengono attivati solo alcuni servizi di base del sistema e quindi é piú difficile che si attivino moduli infetti. A questo punto si puó fare una scansione on-line, questa puó essere anche molto lunga in funzione della quantitá di files, della velocitá di connessione etc... Un modo alternativo e piú veloce consiste nell'usare gli strumenti di scansione forniti da alcune case di antivirus: questi sono spesso immagini ISO da scaricare e copiare su un CD/DVD che contengono un sistema operativo base (spesso Linux) e gli strumenti di rilevazione e rimozione dei virus aggiornati. E' importante utilizzare una versione recente di questi sistemi per evitare di lasciarsi sfuggire un malware recente.
- Se il PC risultasse infetto disconnettere, se possibile, il PC dalla rete per evitare la diffusione dei malware e effettuare una ricerca on-line (magari da un altro PC) per capire quali sono le caratteristiche del malware e come rimuoverlo (ad esempio cercare su google: "nome del virus", rimozione). Spesso le case produttrici di antivirus forniscono specifici strumenti di rimozione per alcuni virus piú aggressivi e diffusi.
- Studiare con attenzione le istruzioni per la rimozione del malware prima di provare a metterle in pratica.
- applicare lo strumento di rimozione e quindi provare a effettuare una nuova scansione (eventualmente online o usando strumenti specifici) per controllare l'effettiva pulizia del sistema.
- Ripristinare il sistema.

1.4 Protezione del PC e norme di comportamento

Alcuni sistemi operativi sono piú esposti di altri all'infezione. Tuttavia un'infezione é spesso colpa di

un comportamento poco prudente da parte dell'utente. Quindi, un comportamento prudente e cosciente é fondamentale per la protezione del proprio sistema. La maggiore espansione di virus su sistemi microsoft non é dovuta, alla maggiore vulnerabilitá dei sistemi windows ma deve essere attribuita alla minore esperienza e maggiore ingenuitá dell'utente medio windows (nel 2005 di circa 5000 vulnerabilitá meno di 1000 sono state osservate su sistemi microsoft, circa 2000 su SO unix/Linux e circa 2000 multi-piattaforma).

Alcune norme di comportamento possono aiutare la prevenzione: **1-Aggiornamento**: aggiornare regolarmente gli antivirus, il firewall e il proprio sistema operativo. Di solito i files delle firme sono aggiornati ogni poche ore sui siti. Attivare l'aggiornamento automatico con periodicitá almeno settimanale. controllare periodicamente i giudizi sul proprio antivirus o firewalll pubblicati sui siti specializati e eventualmente cambiarlo. Attivare gli aggiornamenti automatici del proprio sistema oparativo.

2-Usare software fidato: é bene utilizzare sempre con cautela i siti che forniscono software gratuito. Partendo dal presupposto che chi fa un lavoro la fa, generalmente, per ottenere un guadagno, é sempre bene diffidare dei siti che forniscono gratuitamente software e servizi. Tuttavia il software libero (**freeware**) rappresenta spesso una validissima alternativa a programmi commerciali, ad esempio il diffusissimo pacchetto Open Office (alternativo a Office della Microsoft) o i vari sistemi operativi basati sull'architettura Linux.
Attenzione, il termine freeware indica un software che viene distribuito in modo gratuito, a volte anche con il codice sorgente (in tal caso si parla di open source). Un programma freeware puó essere duplicato e distribuito liberamente, con pochissime limitazioni: in genere si chiede all'utente di rispettare i termini della licenza "GNU General Public License" (www.gnu.org). Esistono diverse banche dati Freeware (sourceforge.net, download.html.it, www.ilsoftware.it, per citarne alcuni) da cui attingere liberamente nei limiti delle licenze pubblicate.
A volte vengono fornite versioni gratuite (freeware) di programmi commerciali (antivirus, firewall, lettori PDF, etc...), queste hanno potenzialitá limitate rispetto alle versioni a pagamento (complete) e sono utili per far conoscere un prodotto e invogliare l'utente all'acquisto di una licenza estesa. A volte queste versioni sono di libero uso solo per periodi limitati. E' bene scaricare questi programmi dai siti ufficiali per evitare copie artefatte, potenzialmente dannose. E' buona norma controllare con attenzione il nome del programma, non é raro che i malware vengono camuffati in programmi con nomi simili a quelli di software commerciali piú famosi.
Alcuni software sono scaricabili liberamente ma chiedono all'utente un contributo relativamente basso per il loro utilizzo o per l'attivazione completa o per evitare noiosi avvertimenti. Sono i cosiddetti shareware, anch'essi diffusi e decisamente validi come alternative a pacchetti commerciali piú costosi.
Prima di installare un nuovo software leggere sempre i termini delle licenze (programmi e utility, gratuiti e non, possono essere utilizzati per raccogliere e diffondere informazioni: accettando i termini della licenza si accetta di comunicare alcune informazioni personali a terzi, non é necessariamente un male ma basta saperlo). Non é raro che un programma "gratuito" contenga codici malware (adware, spyware, trojans) che raccolgono e diffondono informazioni in modo fraudolento. Prima di scaricare e installare un software é bene informarsi, ad esempio visitando blog e commenti di altri utenti, sull'eventuale presenza di malware o malfunzionamenti.

3-Avvio automatico dei dispositivi: Disattivare l'esecuzione automatica dei programmi su CD, DVD e dispositivi USB. Questi supporti sono i vettori piú diffusi per la propagazione di malware. Quando di connette un dispositivo USB a un PC con sistema Windows, a meno che non si tenga premuto il tasto SHIFT il sistema operativo avvia automaticamente le istruzioni contenute nei files *autorun.inf*. Queste istruzioni possono attivare un malware prima che l'antivirus sene accorga. Esistono programmi che permettono di disattivare l'esecuzione automatica da supporti esterni che é bene utilizzare (a meno di non ricordarsi di premere sempre il tasto SHIFT connettendo supporti esterni).

4-Attenzione alle estensioni dei files: visualizzare le estensioni per tutti i tipi di files. Il nome di un file é generalmente composto da un nome seguito da un'estensione, di solito tre lettere (ma possono essere di meno o di piú) dopo l'ultimo punto, ad esempio: *NomeFile.est*. L'estensione indica all'utente e al sistema operativo il tipo di informazioni contenute nel file. Quindi *NomeFile.txt* sono files di testo in formato ASCII, *NomeFile.doc* sono generalmente documenti di office (o altro word processor), *NomeFile.zip* sono documenti generalmente compressi, *NomeFile.xls* sono generalmente documenti di EXCEL, etc...
Nei sistemi windows (e non solo) all'estensione viene associata un'applicazione (programma) che viene usata di default per aprire il documento. Nei sistemi windows l'estensione dei files é nascosta di default. Anche se il tipo di file puó essere comunque riconosciuto dall'icona ad esso associata questo comportamento è poco sicuro (non è un caso che alcuni trojans e worms impediscono di visualizzare le estensioni dei files!) e ignorare l'estensione puó essere pericoloso: files come *NomeFile.bat* (batch files), *NomeFile.com* (macro files), *NomeFile.exe* (programmi eseguibili), contengono istruzioni che vengono eseguite automaticamente al doppio click. Se l'estensione é nascosta é possibile che un'utente distratto attivi le istruzioni

malevoli contenute in un file con un nome innocuo, ad esempio credendolo un file ascii (*NomeFile.txt.bat* puó sembrare un file di testo innocuo: *NomeFile.txt* se si omette l'estensione *bat*), un documento Office o un messaggio. Pertanto é bene modificare le opzioni di sistema per rendere visibile le estensioni per i tutti i files utilizzando le opzioni delle cartelle di windows.

Alcune brevi regole da rispettare:

1. Limitare lo scambio e la trasmissione di files con estensioni come .bat (batch files), .exe (eseguibili), .com (macro), .sys, .inf . Questi files contengono istruzioni che vengono eseguite automaticamente in caso di doppio click. Spesso i programmi di posta, i servers e gli antivirus impediscono la spedizione di messaggi contenenti questi files.

2. Sottoporre a controllo qualsiasi file (di qualunque provenienza) prima di eseguire o leggerne il contenuto (di solito il resident shield e il mail scanner dell'antivirus sono programmati per farlo in modo automatico).

3. Ridurre l'uso di programmi shareware e di pubblico dominio se non se ne conosce la provenienza. Non accettare download da fonti sconosciute. Controllare on-line se ci sono commenti sul software che si intende scaricare e utilizzare.

4. Tenersi informati sulle nuove strategie e sui nuovi comportamenti malevoli, aggiornare regolarmente gli antivirus, firewall e il sistema operativo, Effettuare CONTROLLI PERIODICI con l'antivirus e programmi di supporto (antispyware, etc...).

5. Prestare attenzione a comportamenti "strani" del PC, ad esempio la scomparsa delle estensioni dei files, rallentamenti inattesi, etc...

6. Sviluppare una cultura della sicurezza durante l'utilizzo del computer in modo da diminuire il piú possibile i rischi di infezione da sorgenti interne e/o esterne: lasciare il proprio PC non protetto equivale a lasciare le chiavi sulla propria porta di casa: a volte i vicini possono essere invadenti e poco rispettosi!

7. Imparare come recuperare i propri dati e i programmi dopo un'infezione virale. Sapere dove trovare gli strumenti per la rimozione specifica di malware.

8. Effettuare frequenti backup dei dati e dei programmi critici.

9. In caso di infezione agire con calma, prendendo nota delle varie operazioni effettuate e da effettuare, cercare di contenere l'infezione.

10. **Non seminare il panico inoltrando falsi allarmi ma informarsi sulla veridicitá delle informazioni diffuse**.

1.5 Informazioni on-line

Internet é una fonte di informazioni immensa e preziosa ma va usato con cognizione di causa, tenendo ben presente il fatto che praticamente chiunque puó scrivere qualunque cosa, non necessariamente vera. Le informazioni pubblicate su un sito WEB, su un Blog etc... non sono necessariamente corrette e vanno pertanto verificate di continuo utilizzando le risorse e le informazioni della rete in modo critico. Anche se alcuni siti (ad esempio Wikipedia, siti specializzati etc...) contengono informazioni particolarmente affidabili, il controllo incrociato rappresenta il modo piú efficace per validare le informazioni che si possono reperire in rete.

E' bene avere tra i propri "preferiti" un elenco di siti riguardanti la sicurezza informatica, i software di protezione, strumenti supporto, da consultare in caso di problemi e visitare, di tanto in tanto, per tenersi aggiornati sullo stato dell'arte in fatto di sicurezza, vulnerabilitá, etc...

==========

2 Internet e il WWW

2.1 Reti di calcolatori

Una rete di calcolatori é una struttura in cui piú computers comunicano tra loro scambiandosi dati. Questi computers sono generalmente entitá eterogenee, nel senso che hanno diverso hardware e spesso diversi sistemi operativi. In effetti la rete che chiamiamo Internet, e di cui abbiamo probabilmente un'idea assai vaga, é un'intreccio di reti cui afferiscono sottoreti di calcolatori molto diverse tra loro. Le differenze possono essere nelle dimensioni delle singole reti: wide area network (WAN), metropolitan area network (MAN, ad esempio la rete di PC dell'universitá di Roma TRE), local area network (LAN, ad esempio le rete di PC in casa o in un laboratorio o in un ufficio). Oppure nel supporto usato per le comunicazioni (fibra ottica, ponti radio, cavi coassiali, cavi ethernet, satellite). Oppure possono essere diverse per la topologia cioé lo schema di collegamento dei diversi computers (o nodi), per esempio a stella o ad anello.

Per comunicare tra loro le diverse entitá afferenti a Internet utilizzano un sistema di regole specifiche (protocolli) eguale per tutti che consente uno scambio veloce ed efficiente delle informazioni tra i vari nodi.

Prima dell'avvento di Internet un esempio di "rete" di comunicazione era la rete telefonica che consentiva di scambiare informazione tra due nodi posti in comunicazione diretta tra loro. La rete telefonica (tuttoggi attiva!) é una rete a commutazione di circuito (o indirizzo): il nodo chiamante (telefono) A viene messo in comunicazione diretta con il nodo chiamato (telefono) B tramite diverse centraline che chiudono un circuito elettrico tra A a B. Una connessione di questo tipo é fragile: se si interrompe il circuito A-B cade la comunicazione; é lenta: richiede tempo per effettuare il collegamento diretto; é dispendiosa: richiede un canale di comunicazione attivo ogni due utenti e questo canale deve rimanere attivo anche durante le pause.

Internet si basa su un modello di comunicazione detto a commutazione di pacchetto, ideato principalmente per scopi strategico militari al fine di ovviare alle limitazioni imposte dalle connessioni telefoniche. Il modello a commutazione di pacchetto suddivide il messaggio in *pacchetti* di dati dimensione definita e relativamente ridotta, quindi invia i pacchetti al destinatario individuato da un indirizzo univoco. Ogni pacchetto, oltre alla frazione di messaggio, contiene l'indirizzo di destinazione e tutte le informazioni necessarie e ricostruire il messaggio originale una volta a destinazione. A differenza delle comunicazioni telefoniche i pacchetti, una volta inviati, seguono ognuno una via autonoma passando di nodo in nodo lungo le connessioni che si trovano libere al momento richiesto. Quando un pacchetto giunge su un nodo che non é il suo destinatario viene inoltrato con le stesse modalitá fino a raggiungere la destinazione definitiva. Quando tutti i pacchetti sono a destinazione il messaggio originale viene ricostruito. Una serie di protocolli (regole) stabiliscono come impacchettare i messaggi, come inviarli, come ricostruirli, come segnalare eventuali errori, etc...

Una rete a commutazione di pacchetto é molto piú efficiente di una a commutazione diretta, infatti é poco sensibile a interruzioni della linea: ogni pacchetto segue un percorso autonomo e, in caso di interruzione di alcuni rami, i pacchetti persi possono essere recuperati lungo percorsi alternativi. Inoltre i pacchetti in transito vengono registrati sui nodi di transito, questo facilita la ridondanza dei pacchetti che possono essere reinviati lungo percorsi ottimali. Questo tipo di rete utilizza in modo efficiente la banda di comunicazione: se c'é congestione lungo un percorso alcuni pacchetti possono essere inviati lungo percorsi alternativi; i canali di comunicazione sono diretti, da nodo a nodo, e attivi solo durante la trasmissione. Quindi lo stesso canale puó essere usato nella pause per trasmettere altri pacchetti relativi a diverse comunicazioni. In caso di errori é sufficiente inviare un singolo pacchetto piuttosto che l'intero messaggio.

2.2 Protocolli di comunicazione

E' chiaro che questo tipo di comunicazione richiede regole precise da rispettare in modo automatico. Queste regole sono fissate da protocolli specifici detti "protocolli TCP/IP" in funzione dei due principali protocolli utilizzati per le comunicazioni Internet: TCP (Transmission Control Protocol) e IP (Internet Protocol). Questi protocolli agiscono a diversi livelli: (vedi: it.wikipedia.org/wiki/Suite_ di_ protocolli_ Internet)

- *livello applicazioni*: (es. DHCP, HTTP, HTTPs, SMTP, POP3, FTP, FTPs, ...) sono le regole con le quali i programmi applicativi (browsers, client di posta) si scambiano dati e documenti. Ad esempio stabiliscono come deve essere "tradotto" un messaggio scritto usando Eudora per esser letto da Outlook o Thunderbird. I dettagli dell'impacchettamento della trasmissione sono affidati ai protocolli di livello inferiore.

- *livello trasporto*: il protocollo di trasmissione (es. TCP) mette in coda i messaggi delle applicazioni suddividendoli in pacchetti, li invia e attende una ricevuta di buona ricezione dal destinatario. I dettagli della trasmissione sono affidati ai protocolli di rete.

- *livello rete*: il protocollo IP decide su quale percorso istradare i singoli pacchetti cercando di scegliere la via piú efficiente.

- *livello collegamento* o data-link: sono le regole che stabiliscono come effettuare il trasferimento tra un nodo e l'altro e quale codifica usare. Raggruppa fisicamente i dati in pacchetti, controlla e gestisce gli errori di trasmissione, regola il flusso tra sorgente e destinatario.

- *livello fisico*: sono le regole che stabiliscono l'accesso alla rete fisica ovvero come tradurre il messaggio in impulsi elettrici ottici o radio a seconda del supporto fisico che viene utilizzato.

Per assicurare il collegamento si hanno una serie di indirizzi univoci per individuare i vari elementi della rete:

- MAC-address: individua univocamente le schede di rete (livello collegamento): un PC puó avere piú di una scheda di rete attiva, il MAC-address stabilisce con quale scheda si sta parlando.

- IP-address: individua univocamente un nodo sulla rete (livello rete): individua il computer utente (nodo)

- port-address: individua un numero di "porta" logica sui computer (livello trasporto). La comunicazione avviene attraverso diverse 'porte' logiche, ogni applicazione usa una o piú porte per i dati in uscita e in ingresso.

2.3 Indirizzi IP e URL

I diversi nodi sono indicati sulla rete da un numero univoco che definisce l'IP address. Il formato di questi indirizzi é stabilito in base al protocollo IP (IPv4, attualmente) ed é valore espresso su 32 bit (4 byte) in una sequenza di 4 valori decimali separati da un punto (ed esempio 192.162.37.1). Ogni valore puó essere compreso tra 0 e 255 (8 bit). La parte sinistra di un indirizzo IP individua la rete ed é eguale per tutti i dispositivi di quella rete, la parte destra individua il nodo e individua ogni dispositivo di quella rete in modo univoco. Quando si connette un dispositivo di rete si stabilisce una relazione univoca tra MAC-address e IP-address. Questa associazione puó essere statica (lo stesso indirizzo IP ad ogni connessione) o dinamica (un diverso IP ad ogni connessione). La parte sinistra (indirizzo di rete) viene assegnata da enti e organismi internazionali dietro motivata richiesta.

Chiaramente é piú semplice ricordare nomi e termini mnemonici piuttosto che lunghe serie di numeri, per questo per individuare alcuni nodi di una rete (un determinato server, ad esempio) si usano nomi facilmente identificabili e memorizzabili. I nomi di dominio hanno lo stesso significato degli indirizzi IP e vengono assegnati da organismi internazionali. I nomi di dominio hanno generalmente una struttura gerarchica da sinistra a destra (al contrario di quello che succede nell'indirizzo IP numerico): risorsa.sottodominio.dominio.radice

Per associare l'indirizzo IP numerico al nome simbolico é nato il servizio Domain Name Server (DNS) che, tramite opportuni protocolli, perette di associare ad ogni nome di dominio l'indirizzo IP corretto.

Il World Wide Web (WWW) é la struttura che contiene le "risorse" condivise sulla rete Internet, ovvero le informazioni, i programmi, le basi di dati etc... . L'insieme dei programmi, testi, grafici etc... Il WWW é una struttura di iper-testi in cui sono combinate informazioni testuali, sonore, grafiche, etc... . Le varie risorse sono distribuite sui diversi nodi connessi alla rete e sono collegate e accessibili tramite link (collegamenti). I link sono realizzati utilizzando il sistema delle URL (uniform resource locator) che consente di identificare in modo univoco tutte le risorse disponibili sul WWW. Un indirizzo URL é una stringa composta diversi elementi separati da "/":

http : //webusers.fis.uniroma3.it/ meneghini/CV.html

- **http**: indica il protocollo che si sta usando, in questo caso hyper-text-transfer-protocol. Altri protocolli usati possono essere ftp (file transfer protocol), https (http criptato) etc...

  item **webusers.fis.uniroma3.it** é l'indirizzo IP del computer su cui é localizzata la risorsa

- ∼**meneghini** é la sottodirectory in cui si trovano i dati

- **CV.html** l'oggetto cercato, in questo caso un file html.

Attenzione: il nome del protocollo e l'indirizzo IP possono essere scritti indifferentemente utilizzando lettere maiuscole o minuscole. Il resto della URL é "case-sensitive" ovvero lettere maiuscole o minuscole sono considerate diverse e bisogna prestare attenzione a come viene scritto. Ad esempio:
http://webusers.fis.uniroma3.it/∼Meneghini/CV.html
oppure:
http://webusers.fis.uniroma3.it/∼meneghini/cv.html
non consentono il link alla pagina WEB e, probabilmente, compare un messaggio di errore.