11. Le memorie di massa

Con il termine **memorie di massa** si intendono tutte quelle periferiche nelle quali vengono memorizzati i nostri dati e/o programmi. Tra esse i maggiori rappresentanti sono gli **hard disk** (interni ed esterni), seguiti dai supporti rimovibili come **floppy disc, CD, DVD, pendrive o chiave USB, nastri magnetici, memorie flash** di ogni tipo ed altro ancora.

Vediamoli in dettaglio.

- a. Floppy disk
- b. Hard disk
- c. Pendrive o Chiave USB
- d. Memory card
- e. CD Rom
- f. DVD

12. Periferiche di INPUT

Le periferiche di sistema sono generalmente esterne all'unità centrale e si dividono in periferiche di **Input** e periferiche di **Output**.

Analizziamo le periferiche di Input.

- a. Tastiera
- b. Mouse
- c. Scanner
- d. Altre periferiche di input

13. Periferiche di OUTPUT

Con tale termine si indicano tutte quelle periferiche che ricevono dati dall'unità centrale. Di seguito si indicano le principali.

- a. Monitor
- b. Stampante

14. Sviluppo di un software

Lo sviluppo di un software prevede diverse fasi. Queste possono essere così riassunte:

1. Analisi
2. Progettazione
3. Programmazione
4. Testing o debug
5. Manutenzione

Vediamole in dettaglio.

1. la fase di **analisi**, ovvero l'indagine preliminare sul contesto in cui il prodotto software deve inserirsi, sulle caratteristiche che deve esibire, ed eventualmente su costi e aspetti logistici della sua realizzazione. In senso ampio si può dire che l'analisi ha lo scopo di **definire il problema** da risolvere il più precisamente possibile.

2. la fase di **progetto**, in cui si definiscono le linee essenziali della struttura del sistema da realizzare, in funzione dei requisiti evidenziati dall'analisi e dal documento finale da essa creato. Si può dire che il progetto ha lo scopo di **definire** (a un certo livello di dettaglio) **la soluzione** del problema. In questa fase sarà sviluppato un documento che permetterà di avere una definizione della struttura di massima (architettura di alto livello) e una definizione delle caratteristiche dei singoli componenti (moduli);

3. la fase di **programmazione** o implementazione o *codifica* del sistema, ovvero la sua realizzazione concreta tipicamente consiste nella realizzazione di uno o più programmi in un

determinato linguaggio di programmazione, benché possano essere coinvolte anche tecnologie diverse (database, linguaggi di scripting e via dicendo). Complessivamente, l'implementazione ha lo scopo di **realizzare la soluzione**.

4. la fase di testing o debug costituisce il collaudo. Questa è volta a misurare in che modo il sistema realizzato soddisfa i requisiti stabiliti nella fase di analisi, ovvero a valutarne la correttezza rispetto alle specifiche. In questa fase ritroviamo l'**alpha** ed il **Beta testing** che hanno lo scopo di scovare gli errori (**bugs**) del software. Il primo viene effettuato dai programmatori stessi. Superata questa fase viene iniziata il secondo test che produce quella che viene comunemente definita la versione Beta di un software. La **versione beta** è una versione non definitiva, già testata dagli esperti, messa a disposizione anche dei meno esperti, confidando proprio nelle loro azioni imprevedibili che potrebbero portare alla luce nuovi bug o incompatibilità del software stesso. Più precisamente il **beta testing** (o *beta-verifica*) è una fase di prova e collaudo di un software non ancora pubblicato. Questa operazione può essere svolta da professionisti pagati, oppure, molto spesso, da semplici amatori.
5. la fase di manutenzione, che comprende tutte le attività di modifica del software successive al suo rilascio presso il cliente o la sua immissione sul mercato. Queste attività possono essere volte a correggere errori del software, adattarlo a nuovi ambienti operativi, o estenderne le funzionalità. Si provi ad esempio ad immaginare un software sul calcolo dell'ICI che debba essere aggiornato al variare della normativa.

14. Connettivi logici (And - Or - Not)

A questo punto dobbiamo spiegare meglio come riuscire a formalizzare in maniera logica i concetti che vogliamo trasformare in programma; questa operazione è forse la più importante e complessa, perché è su questa che poi si baserà il lavoro di scrittura del codice che andremo a mettere in atto.
I due strumenti che ci vengono in soccorso sono l'Algebra di Boole (utile per le operazioni sui dati) ed i diagrammi di flusso (utili per rappresentare in maniera ordinata i nostri processi logici).

Apriamo una piccola parentesi sull'Algebra di Boole; questo tipo di logica non è correlata esclusivamente al mondo della programmazione, ma fa parte della vita di tutti i giorni.
Pensiamo ad esempio a quando vogliamo uscire di casa, se piove non possiamo uscire; questo processo mentale, cioè il verificare se piove, può assumere, di fatto, due stati, o è vero (e quindi non usciamo) o è falso (e quindi usciamo). Si può capire che se questo tipo di logica risulta utile a noi come esseri umani, lo è ancora di più per un computer poiché il suo linguaggio è fatto solo di bit ed è possibile associare al vero il valore **1** ed al falso il valore **0**.

L'**Algebra di Boole** verrà qui solamente accennata e sostanzialmente consiste nel prendere come valori "vero" e "falso" (o 1 e 0); posti questi valori andiamo a vedere come operazioni logiche producano dei risultati nuovi e sensati.

AND – Congiunzione

falso AND falso risultato falso
falso AND vero risultato falso
vero AND falso risultato falso
vero AND vero risultato vero

Riusciamo facilmente a comprendere che l'AND restituisce un valore vero "se e solamente se gli altri due valori sono veri", questo vuol dire che anche in una successione di più operazioni AND basta che un valore sia falso ed anche il risultato lo sarà.

OR – Disgiunzione

falso OR falso risultato falso
falso OR vero risultato vero
vero OR falso risultato vero
vero OR vero risultato vero

L'OR invece restituisce un valore vero "se e solamente se almeno uno dei due valori risulta vero"; in poche parole anche in una successione di più operazioni OR basta che un valore sia vero ed anche il risultato lo sarà.

NOT – Negazione

NOT falso risultato vero
NOT vero **risultato falso**

Il NOT si riduce ad una semplice operazione di negazione del valore acquisito.
Si può evincere che grazie all'Algebra di Boole è possibile formalizzare i nostri pensieri riuscendo così a creare strutture complesse di rapido utilizzo, ma che non erano direttamente connesse ai dati iniziali. Basti pensare che i microprocessori stessi si basano sulla semplice logica dell'Algebra di Boole, con la quale è possibile formalizzare qualsiasi tipo di ingresso.

15. Tipi di rete

Le reti vengono divise a seconda della loro estensione geografica in:

- **LAN**: Local Area Network
- **WLAN**: Wireless Local Area Network
- **MAN**: Metropolitan Area Network
- **WAN**: Wide Area Network

LAN

Le LAN (Local Area Network) sono il tipo di rete più ampiamente diffuso negli uffici. Esse si estendono su un piano di un edificio, o su intero edificio. Una LAN si può anche arrivare ad estendersi su più edifici vicini. Caratteristiche peculiari di tale tipo di rete sono:

- Tutti i siti sono vicini tra di loro
- Ampia velocità di trasmissione
- Bassa frequenza di errori
- Costi bassi

WLAN

Le WLAN (Wireless Local Area Network) sono della LAN senza fili.

MAN

Le MAN (Metropolitan Area Network) sono reti che si trovano all'interno di una città o aree metropolitane e gestite da

- Pubbliche amministrazioni,
- Università,
- Reti civiche,
- Agenzie di servizi.

Sono caratterizzate da:

- Alte velocità di trasmissione
- **Costi elevati**

WAN

Le WAN (Wide Area Network) sono nella maggior parte la combinazione di una serie di reti su area locale (LAN) opportunamente connesse tra di loro mediante collegamenti aggiuntivi per permettere la comunicazione tra di loro. Sono nate per collegare tra di loro siti di ricerca distanti tra di loro e sono caratterizzate da:

- Costi bassi
- Velocità basse
- Utilizzano linee telefoniche standard come mezzo di comunicazione principale

16. INTERNET, INTRANET, EXTRANET

Internet, denominata anche ***rete delle reti***, è la più grande rete telematica mondiale che permette a miliardi di elaboratori di comunicare tra di loro. Poiché essa è in grado di connettere computer in tutto il mondo viene definita anche ***rete globale***. Dunque Internet che vuol dire "Interconnected Networks" cioè "*reti connesse tra loro*" è un sistema di collegamento tra computer e reti di computer, che ne permette la comunicazione diretta per scambio di informazioni e/o servizi.

Esistono però numerose piccole "internet private" ad accesso controllato, chiamate Intranet, gestite e utilizzate internamente da società e aziende. Quando una parte della intranet viene resa accessibile a clienti, partner o altre persone esterne all'organizzazione, si ha una Extranet.

17. World Wide Web

Il World Wide Web ha iniziato ad avere diffusione all'inizio degli anni 90 sulla spinta del protocollo HTTP. Attualmente è noto come WWW, W3 o semplicemente Web: in ogni caso sono sinonimi del World Wide Web. Infatti il WWW non è altro che una vasta rete di server HTTP in grado di comunicare tra di loro grazie ad Internet. Il Web non è Internet: è solo uno dei servizi che è possibile trovare su Internet. Attualmente il temine usato dagli utenti del Web per indicare che si consultano documenti sulla rete è navigare (in inglese surfing).

18. Servizi di Internet

Internet ha avuto una larghissima diffusione grazie all'enormità di servizi messi a disposizione anche se alcuni sono disponibili o meglio apprezzabili solo in presenza di connessioni DSL (definite, anche se erroneamente, a banda larga). Vediamo di conoscerne i principali.

Alcuni dei servizi presenti da diverso tempo, che tutti conosciamo o perlomeno ne abbiamo sentito parlare, sono:

- **E-Mail** (posta elettronica)
- **Chat Line**, **Newsgroup**, **Forum** (conversare con persone o un gruppo di persone)
- **E-Commerce** (commercio elettronico on line)
- **Home-Banking** (gestione del proprio Conto corrente on-line)
- **E-Government** (processo di informatizzazione della pubblica amministrazione che attraverso l'uso delle tecnologie informatiche tendono ad ottimizzare il lavoro degli enti ed offrire agli utenti servizi più rapidi)
- **E-Learning** (apprendimento a distanza attraverso la rete internet)
- Il **telelavoro** indica una attività del lavoratore che viene normalmente svolta, con l'ausilio di strumenti informatici ed attrezzature telematiche, in luogo diverso dai locali aziendali, prevalentemente da casa.
- La **telemedicina** è la possibilità di curare un paziente a distanza o più in generale di fornire servizi sanitari a distanza grazie all'utilizzo di tecniche mediche ed informatiche.
- **IPTV** (**Internet Protocol Television**) rappresenta la possibilità di utilizzare internet per veicolare contenuti audiovisivi in formato digitale. In realtà questo servizio presumo sia stato già superato, ad esempio da Youtube.
- La **teleconferenza** è la possibilità che permette a più individui di eseguire comunicazioni audio-video, dai vari luoghi nella quale essi sono dislocati, attraverso internet.
- La **videochiamata** è la possibilità di poter dialogare con un telefono che permette anche la visualizzazione dell'immagine.
- **Voice over IP** (Voce tramite protocollo Internet), acronimo VoIP, indica l'utilizzo di una normale conversazione telefonica attraverso la connessione Internet.
- **IM (instant messaging- Messaggistica istantanea)** scambio in tempo reale tra due utenti di brevi messaggi di testo. Molto usata in software quali Skype, MSN o su Facebook.

- **Feed RSS** (**flussi RSS**) rappresentano la possibilità di creare informazioni su qualsiasi argomento che l'utente potrà vedere molto comodamente, con l'aiuto di un lettore apposito, nella stessa pagina, nella stessa finestra, senza dover andare ogni volta nel sito principale che ha generato quell'informazione.
- un **blog** è un diario personale on-line pubblicato su un sito internet e generalmente gestito da una persona che periodicamente aggiorna con opinioni personali, descrizione di eventi, o altro materiale come immagini o video. In esso è possibile permettere a eventuali visitatori di lasciare i propri commenti o le proprie opinioni sull'argomento.
- Un **podcast** altro non è che un Feed RSS al quale si è aggiunto un contenuto audio e/o video. In pratica è un **programma radio o video** registrato digitalmente e reso disponibile su Internet.

19. Modi di connessione a Internet

Vediamo adesso di capire come ci si collega a internet.

Le aziende che ci offrono la possibilità di accedere a internet prendono il nome di **ISP** (Internet Service Provider). Quando si stipula un contratto con questi affittiamo un computer che ci riconosce ogni volta che vogliamo accedere al servizio e ci permette di connetterci alla rete.

Perché ciò possa avvenire è necessario che il nostro PC sia connesso ad un modem/router . In base alle caratteristiche di quest'ultimo si ha il tipo di connessione. (vedi la voce **modem**).

È chiaro che un modem tradizionale ISDN non potrà funzionare su una connessione ADSL e viceversa.

Di seguito un breve riepilogo delle varie modalità di connessione a internet (per approfondimenti vedi alla voce modem).

- **Linea telefonica;**
- **Telefono cellulare;**
- **Cavo;**
- **Wireless: WDSL** (Wireless DSL) è una tecnologia di rete nell'ambito delle telecomunicazioni senza filo che offre la possibilità di usufruire della tecnologia ADSL via wireless nei comuni ove non è presente la linea ADSL;
- **satellite:** La qualità del servizio Internet via satellite è notevolmente peggiore di una connessione ADSL.

L'utente per ottenere una qualsiasi delle su esposte linee dovrà pagare una tariffa che può essere : **Flat** o **free**.

Nella free non vi è alcun costo del canone ma l'utente paga per il tempo di effettiva connessione al servizio;

nella flat invece viene corrisposto all'ISP un canone mensile di abbonamento che permette di rimanere connessi anche 24 ore al giorno.

Un caso a parte merita la connessione denominata "**Internet mobile**" diffusasi ultimamente che permette di accedere al servizio direttamente dal telefonino o con un PC (fisso o portatile) collegato ad un telefonino, o con una Internet Key.

Le tariffe in questo caso sono a volume e a tempo. Entrambi prevedono una tariffazione differenziata, le prime per quantità di dati scaricati, mentre le seconde per il tempo di connessione.

20. Protocolli

Un protocollo è un insieme di regole che stabiliscono come deve avvenire uno scambio di dati tra due o più elaboratori.

Su Internet vengono usati, a scopi diversi, un gran numero di protocolli, che nel loro complesso sono generalmente indicati come **protocolli TCP/IP** (anche se il nome corretto, che nessuno usa, è **Internet Protocol Suite** ossia *collezione di protocolli Internet*).

È allora necessario conoscere almeno i più comuni per poter accedere a *tutte* le informazioni normalmente reperibili sulla rete.

TCP (Transfer Control Protocol) e **IP** (Internet Protocol). Il primo definisce il controllo delle comunicazioni fra le reti; IP gestisce le trasmissioni utilizzando pacchetti di dati su reti Ethernet. I

dati da inviare, suddivisi nel nodo di partenza in pacchetti che possono seguire cammini diversi attraverso la rete, vengono ricomposti nel nodo di arrivo. Il vantaggio di questo sistema consiste nel fatto che non è necessario né definire né conoscere il percorso, perché è il software che si preoccupa di instradare i dati lungo il cammino più veloce.

HTTP (HyperText Transfer Protocol) Trasferimento di ipertesti e altri file nell'ambito del WWW

FTP (File Transfer Protocol) Copia di file binari o di testo (ASCII)

Telnet protocollo per il controllo di computer a distanza

SMTP (Simple Mail Transfer Protocol) Spedizione di messaggi di posta elettronica (E-mail)

POP3 (Post Office Protocol 3*)* Ricezione dei messaggi di posta in arrivo.

Oltre a questi, con l'avvento dei cellulari si sono imposti anche altri protocolli legati a quest'ultimi. Essi sono: **GSM**, **WAP**, **GPRS, EDGE** e **UMTS**. Vediamoli più da vicino.

GSM (Global System for Mobile Communications) permette di inviare e ricevere dati per i cellulari di seconda generazione.

WAP (Wireless Application Protocol) permette di inviare e ricevere dati tramite dispositivi senza fili.

GPRS (General Pack Radio Service) non è altro che la gestione del protocollo di Internet tramite rete GSM. In pratica consiste nella possibilità, per i telefonini, di ricevere e scambiare dati in Internet alla velocità massima di 171 Kbps.

EDGE (Enhanced Data GSM Environment) Evoluzione del GPRS che permette di raggiungere una velocità massima in trasmissione di 384 Kbps.

UMTS (Universal Mobile Telecommunication System) sistema per la trasmissione dati di terza generazione. Questo protocollo, ci offre la possibilità di effettuare o ricevere videotelefonate oltre che di collegarci a Internet ad una velocità di 2Mbps circa.

21. Sicurezza informatica

Connettersi ad altri computer all'interno di una LAN (casalinga o aziendale) per condividere un documento, navigare sulla rete alla ricerca dell'offerta del mutuo più conveniente o dell'ultima versione di un software da scaricare, ricevere una comunicazione nella propria casella di posta elettronica sono ormai diventate azioni comuni grazie all'utilizzo sempre più crescente del PC sia in casa propria che sul posto di lavoro.

D'altra parte, al di là degli innegabili vantaggi che l'era telematica ha apportato alle nostre abitudini di vita e lavorative, esistono anche altri aspetti da considerare ed, in particolar modo, quelli legati all'esistenza di una serie di "rischi" che possono derivare dall'espletamento di una tra le tante attività precedentemente citate a titolo soltanto esemplificativo.

Le fonti di questi rischi potenziali possono essere veramente molteplici: dai **virus informatici**, ormai creati in quantità industriali, al codice alterato scaricato da qualche sito "corrotto" fino ad arrivare, nel peggiore dei casi, all'intromissione nel nostro sistema di un **hacker** o peggio all'azione distruttiva di qualche **cracker**.

Indubbiamente non è facile rendersi conto della complessità e della vastità della problematica oggi comunemente nota con il nome di Sicurezza informatica, ma è evidente che quest'ultima non può più essere né trascurata né sottovalutata da parte di chi usa un PC per un scopo non soltanto ludico.

Cercheremo di illustrare i pericoli insiti in tale attività e le possibili armi di difesa.

22. Malicious software e Malware

Le cronache informatiche di questi ultimi tempi hanno fornito la dimostrazione pratica di un dato di fatto innegabile: nessuno può dirsi veramente al sicuro dagli attacchi portati attraverso il cosiddetto **codice nocivo**. Ma che cosa si intende per codice nocivo ed in quale modo questo può effettivamente produrre un danno ?
Il termine inglese è **malware**, contrazione di **malicious software**, con il quale, generalmente si intende un qualsiasi frammento di codice (in pratica un piccolo programma) di lunghezza variabile

che, penetrato all'interno di un computer, si dimostra potenzialmente in grado di danneggiarne i dati e/o comprometterne la sicurezza.
Dunque la caratteristica che giustifica l'appellativo di nocivo è l'attitudine a causare danni a prescindere dalla circostanza che poi questi effettivamente si verifichino. Per questo motivo in questa categoria rientrano anche i tradizionali **virus**.
La RFC 1135 definisce come virus qualsiasi porzione di codice che si installa all'interno di un programma host al fine di utilizzare quest'ultimo come mezzo di propagazione. Un virus non può essere eseguito in maniera autonoma ed indipendente ma richiede che sia stato attivato un programma host.
Due sono gli elementi che è necessario prendere in considerazione quando si parla di virus: il **meccanismo di propagazione** ed il **tipo di operazioni eseguite** una volta che il virus sia attivo e residente in memoria. Il meccanismo di propagazione è forse l'aspetto più importante nel valutare la pericolosità di una determinata classe di codice nocivo.
Infatti mentre in passato il pericolo di una infezione da virus poteva dirsi limitato a pochi pc ed il mezzo di diffusione era costituito principalmente da floppy disk o da cassette attualmente l'avvento di Internet ha dato un forte impulso alla crescita delle infrastrutture di rete per cui negli scenari odierni i danni causati dai virus possono colpire centinaia di migliaia di sistemi in poco più di una settimana sfruttando mezzi di connettività globale velocissimi come ad esempio la posta elettronica.

Tra le varie tipologie di virus troviamo:

i **boot virus**, che infettano il **Boot Sector** o il **Master Boot Record** dei dischi (vale a dire quell'insieme di istruzioni localizzate all'inizio di qualsiasi disco fisso, cioè nel primo settore del primo cilindro del primo piatto, in grado di interpretare la tabella delle partizioni che contiene la mappa della configurazione dell'intero disco) in modo da essere caricati all'avvio del sistema. Peraltro, nel gruppo, è proprio questa tipologia di virus quella che presenta le particolarità più insidiose in quanto tende ad acquisire il controllo dell'MBR rilocandolo altrove ed inserendo il proprio codice nocivo all'interno dello stesso. In questo modo, durante il **riavvio della macchina**, il virus riesce ad eseguire qualsiasi tipo di operazione: modificare le chiamate del BIOS od intercettare quelle dirette a leggere lo stesso MBR dirottandole verso la copia precedentemente rilocata (l'uso di queste tecniche cosiddette **stealth** è normalmente diretto ad evitare l'identificazione da parte dei normali antivirus). In pratica si dimostrano particolarmente subdoli poiché sono in grado di acquisire il controllo del sistema al momento del suo bootstrap e quindi molto prima che sia caricato il sistema operativo e, conseguentemente, qualsiasi programma antivirus;

i **file virus o virus di tipo parassita**:, che infettano, con modalità molto varie, i file perlopiù eseguibili (.com, .exe e .dll) e utilizzano lo scambio di questi ultimi per propagare l'infezione lasciandoli perfettamente utilizzabili ma al tempo stessi utilizzandoli come mezzi di propagazione. Quando l'utente o il sistema avviano il *file* eseguibile ospite, avviano anche il virus che viene caricato in memoria e inizia l'attività di propagazione;

i **macrovirus**, che sono generalmente script incorporati all'interno di particolari documenti (come ad esempio un documento di Microsoft Word o di Excel) i quali comprendono una serie di comandi codificati in base al linguaggio specifico di una determinata applicazione che generalmente è il VBA (Visual Basic for Application). Per la prima volta nella storia questi virus hanno sovvertito un punto fermo rappresentato dal fatto che, in passato, non era possibile concepire del codice virale in una forma tale che potesse **prescindere dall'esistenza di un file eseguibile** mentre oggi tutto questo è divenuto realtà proprio grazie alle accresciute potenzialità che nel tempo queste applicazioni sono venute ad acquisire. Indubbiamente alcuni degli esempi più lampanti di questa tipologia di codice è rappresentato dal macro Virus denominato **Melissa** e **Iloveyou** che recentemente sono assurti alle cronache informatiche per la loro rapida diffusione nonché per il semplice ma efficace stratagemma che essi usavano per replicarsi. Come se ciò non bastasse entrambi i virus erano in grado di propagarsi auto inviandosi il primo ai primi 50 indirizzi ed il secondo a tutti gli indirizzi presenti nella rubrica di Microsoft Outlook, sfruttando in tale modo un mezzo di diffusione straordinariamente veloce come la posta elettronica;

i **network virus o Worm**, che si diffondono sfruttando le vulnerabilità dei protocolli di Internet.

23. L'uso di tecniche evolute nei moderni virus

L'evoluzione delle tecniche di programmazione ha portato negli ultimi anni alla proliferazione di una nuova generazione di codice virale sempre più insidioso e subdolo rappresentato da:

- virus polimorfici;
- virus crittografati;

La **prima specie** raccoglie quei virus che adottano tecniche particolari per rendere la loro impronta virale diversa di volta in volta. Attraverso un complesso e sofisticato processo di recodifica essi creano delle varianti di se stessi ostacolando o rendendo molto più difficoltosa la loro identificazione da parte dei programmi antivirus.

Il **secondo genere** invece si caratterizza per l'utilizzo di metodi di occultamento della impronta virale che sfruttano la crittografia. In questo caso la logica di crittografia/decrittografia può essere contenuta all'interno dello stesso codice virale oppure può impiegare apposite routine fornite di default dallo stesso sistema operativo limitando tuttavia in questo caso la propria capacità offensiva soltanto ad tipo sistema (quello di cui vengono sfruttate le API crittografiche).
Peraltro nulla esclude l'impiego congiunto di polimorfismo e crittografia al fine di produrre virus altamente evoluti anche se ciò inevitabilmente si traduce in un codice di maggiori dimensioni la cui realizzazione è alla portata di pochi individui in possesso di capacità tecniche non comuni.
Accanto ai virus sopra citati troviamo altri "programmini" che non sono dei veri e propri virus ma rientrano tra i malware e, dunque, rappresentano una qualsiasi potenziale minaccia.

Questi sono:

Adware che fondamentalmente è ogni software che visualizza pubblicità sul tuo computer. Sebbene l'adware di per sè non rappresenti una minaccia alla privacy o alla sicurezza, i fattori sottoposti a controllo che lo rendono nocivo sono ad esempio:
Sicurezza - se l'adware si installa a vostra insaputa, o è menzionato soltanto a pagina 24 di una lunga licenza d'uso senza alcuna opzione per evitare la sua installazione.
Connettività - se l'adware installa una sua propria procedura di aggiornamento automatico che scarica aggiornamenti e/o software aggiuntivo senza la vostra conferma o addirittura a vostra insaputa.
Persistenza - se l'adware rimane residente in memoria e vi infastidisce con messaggi pubblicitari, perfino se l'applicazione ospite che lo aveva installato non è in esecuzione, e ciò non è stato dichiarato al momento dell'installazione.
Backdoors - se la rimozione dell'ospite non rimuove l'adware, e l'adware utilizza schemi di protezione multipli per impedire la propria rimozione.

BHO che sono piccoli programmi che estendono le funzionalità del proprio browser non rappresentando alcuna minaccia. Alcuni di essi, però, si installano segretamente per spiare il vostro utilizzo del browser, oppure rendono instabile quest'ultimo nel quale sono integrati (ad es. Internet Explorer), lo mandano in crash o sono causa di altri effetti collaterali negativi.

Hijackers - Dirottatori del Browser che in pratica sono dei software che modificano la pagina iniziale o di ricerca del browser cercando di impedirvi di ripristinare le impostazioni personali.

Dialer: qualsiasi software progettato per chiamare numeri a pagamento per scopi frivoli utilizzando l'hardware telefonico (ad esempio siti porno o di download sonerie o altro)

Keylogger: sono programmi progettati per spiare le altre persone attraverso l'intercettazione dei tasti premuti sulla tastiera.

Spyware: Lo Spyware rappresenta la forma peggiore di adware. Generalmente lo spyware coincide con gli stessi criteri usati per l'adware con l'aggiunta di uno o più dei seguenti:
Tracciamento - il monitoraggio del traffico Internet rivela che il programma trasmette un'identificativo univoco assegnato a voi / al vostro computer, per tracciare le vostre abitudini di utilizzo del software o altro.
Spionaggio - il traffico Internet rivela che vengono trasmesse informazioni personali, per esempio gli URL completi o dati inseriti in moduli, compresi possibili dati sensibili quali nomi e password di connessione.
Dichiarazioni vessatorie - la Dichiarazione sulla Privacy del prodotto rivela che vengono raccolte informazioni personali, che talvolta vengono anche vendute.
Dichiarazioni equivoche - se la Dichiarazione sulla Privacy asserisce che viene trasmessa soltanto qualche innocua informazione non-personale, senza escludere esplicitamente ogni dato personale come invece fanno le Dichiarazioni sulla Privacy serie.

Tra gli spyware rientrano i **cookie** traccianti. I cookie (letteralmente significa biscottino) sono utilizzati un po' dappertutto su Internet in posti più o meno utili. Le agenzie pubblicitarie spesso impostano i cookie allorquando il tuo browser carica un banner da una loro pagina. In questo caso e se il cookie contiene un identificativo personale GUID (un identificatore alfanumerico univoco) al fine di effettuare analisi statistiche complessive, autenticare i visitatori e/o personalizzare prodotti e servizi, o ottenere informazioni riguardo ai siti da te visitati e altro.

Trojan: richiamando la guerra di Troia, nell'Iliade di Omero, nella quale la città viene espugnata dai greci grazie allo stratagemma del famoso *cavallo di Troia*, questo malware indica un software che si installa a nostra insaputa nel nostro computer per cedere il controllo della macchina al malintenzionato che generalmente effettua azioni nocive. A volte è spesso un programma che inganna, dichiarando di svolgere determinate funzioni, per di più di utilità, ma che in realtà non fa. Di solito tale classificazione è accompagnata da quella di keylogger, spyware o virus, che definisce il livello di minaccia rappresentata dal trojan.