Contenuti

- Architettura di Internet
- Principî di interconnessione e trasmissione

Tecnologie delle reti di calcolatori

- World Wide Web
- Posta elettronica
- Motori di ricerca

Servizi Internet (*come funzionano e come usarli*)

- Antivirus
- Personal firewall

Servizi Internet (*come difendersi*)

Come comportarsi, quali sono i rischi e come difendersi

- **Nell’uso della posta elettronica**
- **Nell’uso del Web**
- **Nell’uso di altri servizi di rete**

Premessa

- **Ci sono centinaia di milioni di utenti collegati in rete**
- **Tutti, potenzialmente, possono comunicare con il TUO computer collegato in rete**

- **La brutta notizia è che… ciascuno di questi utenti può bussare alle "porte" del tuo computer per vedere se qualcuna è "aperta"**

Porte e indirizzi

- **Con l'indirizzo IP si identifica un computer e il segmento di rete su cui esso si trova, ma è necessario che anche le applicazioni installate sul computer possano essere identificate**
- **Il numero di porta identifica l'applicazione installata sul computer**
  - Porta = numero intero
- **Ad ogni applicazione che deve inviare e ricevere dati dalla rete viene assegnato un determinato numero di porta**
  - ES: la porta 80 è utilizzata dai server Web, mentre la porta 53 viene utilizzata dal sistema DNS

Backdoor

- **Le *backdoor* sono paragonabili a *porte di servizio* (porte sul retro) che consentono di superare in parte o in tutto le procedure di sicurezza attivate in un sistema informatico**
- **Possono essere intenzionalmente create dai gestori del sistema informatico per permettere una più agevole opera di manutenzione dell'infrastruttura informatica, ma più spesso da hacker intenzionati a manomettere il sistema**
- **Possono essere installate autonomamente da alcuni *virus*, in modo da consentire ad un utente esterno di prendere il controllo remoto della macchina senza l'autorizzazione del proprietario**

Possibili conseguenze di un "computer compromesso"

1. **Conseguenze sul tuo computer**
   - Difficoltà operative
   - Controllo/furto/danneggiamento di email (incluse liste di indirizzi) e documenti
   - Controllo e possibilità di transazioni finanziarie illecite (a tuo nome)
   - Furto di identità (nuova frontiera negli USA)
2. **Uso criminale del tuo computer per altri fini (*potrebbe essere penalmente rilevante*)**

Come te ne accorgi

Vedi sul monitor ...

- Uno schermo blu, oppure figure strane o messaggi incomprensibili, ovvero messaggi di errore di sistema

Sperimenti…

- Ritardi inusuali nella fase di avvio del computer
- Computer che “va estremamente lento”
- Presenzi di (molti) file corrotti, inaccessibili o mancanti
- Impossibilità di accedere ai dati sul disco o al disco stesso (quindi a tutti i dati)
- Improvvisi (e frequenti) messaggi di memoria insufficiente
- Riavvio spontaneo del computer

Ma potrebbe anche darsi che non sperimenti alcun sintomo e sei del tutto inconsapevole che il tuo computer è stato compromesso

7

Possibili conseguenze

A seconda del tipo di danni causati, i virus possono essere:

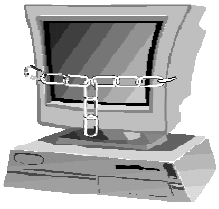
- ***Fastidiosi ma non dannosi*: se comportano solo una diminuzione dello spazio libero sul disco**
- ***Dannosi*: se provocano problemi alle normali operazioni del computer (ad esempio, cancellazione di alcune parti dei file);**
- ***Molto dannosi*: se causano danni difficilmente recuperabili come la cancellazione di informazioni fondamentali per il sistema (formattazione di porzioni del disco)**

La buona notizia

La maggior parte di incidenti può essere prevenuto

Cosa fare?

- **Essere preparati a:**
  - **Proteggersi (“Protect”)**
  - **Riconoscere (“Detect”)**
  - **Reagire (“React”)**



Errori comuni

- **Uso di password “banali”**
- **Aprire attachment di email da sconosciuti**
- **Mancata installazione di software anti-virus**
- **Condivisione di informazioni (password e account)**
- **Mancata segnalazione di violazioni di sicurezza**
- **Mancato aggiornamento del sistema operativo (*patches di sicurezza*) e del software antivirus**

Account e Password: consigli

- **Scegliere una password che non può essere indovinata** (es., un acronimo di una frase con qualche numero inserito a caso) **e con un buon livello di sicurezza**
  - Siti che controllano il livello di sicurezza della vostra password: www.passwordmeter.com
- **Cambiare la password almeno 2-4 volte all’anno**
- **Usare il *desktop locking* durante il giorno** (es., uno screen saver con password per il ri-accesso)

Back-up

- **Salvare periodicamente (almeno) i file più importanti su un supporto diverso dal disco fisso usato normalmente, in modo che possano essere ripristinati nel caso si verificassero perdite o danneggiamenti di dati**
- **Verificare periodicamente l'integrità dei file di copia salvati** (per evitare brutte sorprese…)
- Windows fornisce l'utilità di backup: Start → Programmi → Utilità di sistema → Backup

Modulo 1:
Sicurezza nella posta elettronica

Aprire o no un attachment?

- **Chiedersi se è il caso di aprire un allegato (*attachment*) dal testo della mail, dallo scopo e dal mittente**
  - Attachment di un email che non è collegata a motivi di lavoro o a persone note
  - Attachment con un'estensione sospetta (es., *.exe, *.vbs, *.bin, *.com, o *.pif)
- **REGOLA: Se l'attachment è sospetto, non aprirlo!**
  - Un allegato non aperto non è pericoloso
  - L'apertura di un allegato aperto può provocare l'esecuzione di un virus sul vostro sistema

Sicurezza nell'email

- **Cancellare tutti i messaggi da parte di persone non note che invitano a "cliccare" su di un link Web SENZA CLICCARE**
  - Potrebbe scaricare direttamente qualcosa sul vostro pc
  - Potrebbe segnalare che il vostro account di email è attivo
- **Cancellare tutte le email di pubblicità non richiesta SENZA RISPONDERE (no reply)**

  RICORDARSI che le istruzioni riportate "to remove you from the mailing list" spesso servono per conferma che l'account di email è funzionante

SPAM

- **Origina dal titolo di un popolare sketch del gruppo comico inglese dei Monty Python (la carne in scatola Spam)**

➔ **Azione di diffondere a utenti di posta elettronica messaggi pubblicitari non desiderati**

In generale, si considera SPAM qualsiasi email non richiesta e non desiderata

- **Consuma tempo (per eliminarla) e spazio su disco**
- **Costa milioni di dollari ai grandi provider (traffico)**

Cosa può essere considerato Spam?

- **Se ricevo notizie di un evento/conferenza che mi interessa è spam?**
- **Volume e frequenza dei messaggi: quando diventa spam?**
- **…**

Perché lo SPAM?

Basta fare un po' di conti …

- Inviare email spam a circa 100 milioni di mailbox
- Se anche solo il 10% legge la mail e clicca sul link ➔ si raggiungono 10 milioni di persone
- Se 1% delle persone che va sul sito, sottoscrive per esempio all'offerta di prova per 3 giorni ➔ (100,000 persone) x ($0.50) = $50,000
- Se l'1% della offerta di prova, si iscrive per 1 anno ➔ (1,000 persone) x ($144/anno) = $144,000/anno

Cosa fare?

- **NON RISPONDERE MAI NE' CHIEDERE DI ESSERE ELIMINATI DALL'ELENCO**
- **Non rispondere alle email che richiedono dati personali**
- **Non comprare niente che ha origine da una email spam**
- **Non inoltrare messaggi di "catene di email"**
- **Controllare se l'ISP ha in atto provvedimenti o spazi adatti per la gestione dello spam**

➔ USO DI PRODOTTI ANTISPAM

Modulo 2:
Altri rischi

Rischi

- **PHISHING**
- **HOAX**
- **VIRUS**
- **SPYWARE**

Malware
- Contrazione di ***malicious software***
- Qualsiasi software creato con lo scopo di causare danni al computer su cui viene in installato o all'utente che lo riceve
- Non sono nati a causa di Internet, ma certamente lo sviluppo di Internet ne ha aggravato il potenziale di diffusione

Phishing

- **Non è un malware, ma è una delle modalità fraudolente usate per ottenere informazioni personali**
- **Può capitare a chiunque…**
- **Vedere http://www.antiphishing.org per una interessante serie di esempi.**

Esempio di phishing

Need Help?

Dear eBay User,

We regret to inform you, that we had to block your eBay account
because we have been notified that your account may have been compromised by outside parties.

Our terms and conditions you agreed to state that your account must always be under your control or those you designate at all times. We have noticed some activity related to your account that indicates that other parties may have access and or control of your information in your account.

Please be aware that until we can verify your identity no further access to your account will be allowed.As a result,Your access to bid or buy on eBay has been restricted.To start using your eBay account fully,Please uptake and verify your information by clicking below

http://signin.ebay.com/aw-cgi/eBayISAPI.dll?Verify

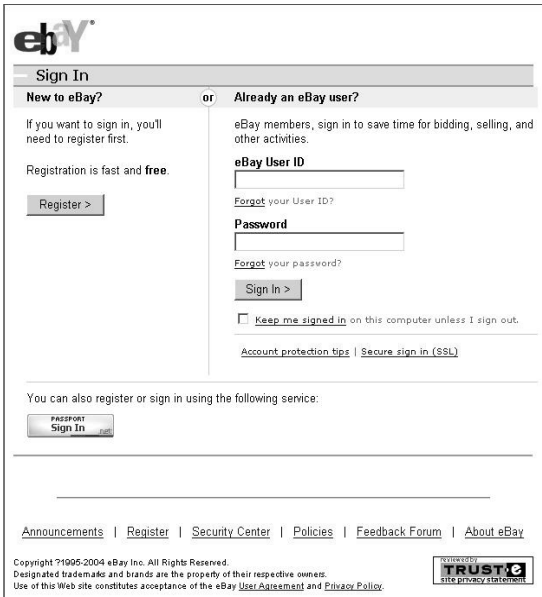
Regards,

eBay Member Service

Please Do Not Reply To This E-mail As You Will Not Receive A Response

Announcements | Register | Safe Trading Tips | Policies | Feedback Forum | About eBay

Esempio di phishing



HOAX

Bufala o falso allarme: tentativo di ingannare il pubblico

Chain Letters (In Italia, nota anche come “Catena di Sant’Antonio”) – Una mail che richiede al destinatario di inoltrarla al maggior numero di persone che conosce (spesso collegata a record, opere caritatevoli, promozioni commerciali, …)

Virus Hoax – Un caso particolare del precedente: mail di allerta che avvisa di un nuovo pericolosissimo virus. Richiede all’utente di diffondere l’avviso al maggior numero di persone che conosce

➔ Il pericolo è la mail stessa! Non perché contiene un virus, ma perché tende ad intasare le mailbox

Virus

- **I virus informatici sono dei programmi (tipicamente molto piccoli) che sono in grado di replicarsi copiandosi in altri programmi o in particolari sezioni del disco fisso, in modo da essere eseguiti ogni volta che i file infetti sono aperti; si trasmettono da un computer a un altro tramite allegati o spostamenti di file ad opera degli utenti**
- **I primi sintomi di malfunzionamento o funzionamento diverso dal normale dovrebbero mettere in allerta**
- ***Come nel caso dei virus non informatici, la prevenzione e l'intervento tempestivo sono la medicina migliore***

Altri tipi di malware

- **Bomba logica: si presenta come una qualsiasi applicazione informatica, ma ha al suo interno una funzione ostile che, tipicamente, si attiva dopo un certo tempo. Può essere molto distruttivo (es., cancellare l'intero contenuto del disco)**
- **Cavallo di Troia: Programma collegato ad un altro file o programma innocuo, che viene scaricato o installato dallo stesso utente. Contiene però istruzioni dannose per cui, una volta installato sul computer, può avere effetti dannosi.**
  - **Es: informare il creatore quando si attiva una connessione Internet, consentendogli di accedere al computer stesso (in modo manifesto, distruttivo, o anche in modalità nascosta)**

Altri tipi di malware

- **Worm ("verme"):** categoria particolare di malware in grado di autoreplicarsi: a differenza dei virus non hanno bisogno di infettare altri file per diffondersi, perché **modificano il sistema operativo stesso** della macchina ospite in modo da essere eseguiti automaticamente ad ogni avvio
- **La replicazione avviene spesso tramite Internet** con diverse modalità:
  - **Posta elettronica**: ricerca indirizzi email memorizzati nel computer ospite e invio di una copia del worm come file allegato (*attachment*) – spesso cammuffato come non eseguibile

Altri tipi di malware

- **Sfruttamento di "bug" di programmi**: Es: i bug consentono all'allegato di eseguirsi automaticamente al momento della visualizzazione del messaggio email
- **Falsificazione dell'indirizzo mittente**
- **File sharing**: i worm si copiano tra i file condivisi dall'utente vittima, spacciandosi per programmi ambiti o per crack di programmi molto costosi o ricercati, in modo da indurre altri utenti a scaricarli ed eseguirli

SOLUZIONE

- **NON CI SONO ALTERNATIVE!!!**

  Bisogna installare un antivirus e bisogna tenerlo continuamente aggiornato

Azioni da compiere

- **L'anti-virus è indispensabile sia per proteggere noi dagli altri sia per proteggere gli altri da noi**
- **Nota dolente: con la diffusione continua di nuovi malware, purtroppo, non si può essere mai sicuri che non si verrà infettati**
- **Tuttavia, si possono ridurre le probabilità di infettarsi**
  →Prendendo continuamente nuovi "vaccini"
- ***La frequenza giornaliera nell'aggiornamento non è da "paranoici"…***

SPYWARE

- **Spyware è un termine generale con cui si definisce un *software utilizzato per scopi fraudolenti* atti a:**
  - Reperire informazioni (personali, password, numero carta di credito, software utilizzato, ecc.)
  - Modificare la configurazione del computer
  - Tracciare tutte le azioni dell'utente o tracciare solo l'uso di determinati servizi Internet (es., pagine Web visitate) per scopi pubblicitari o altro

Tutto senza chiedere il consenso

Problemi con Spyware

- ***Software che raccoglie informazioni su di te e sull'uso del tuo computer***
- ***In alcuni casi potrebbe quasi non essere negativo***
  - Es., Ti iscrivi ad un servizio di musica, lo spyware prende nota, e arriva molta più pubblicità di natura musicale
- **La maggior parte, tuttavia, ha scopi molto negativi:**
  - Raccogliere le password, numero di carte di credito, conto corrente, ecc.

ESEMPIO

Programmi Toolbar → una volta installati, possono essere configurati per raccogliere qualsiasi informazione: tasti battuti, siti Web visitati, nomi e password

ANCHE SE VENGONO RIMOSSI, lasciano delle "briciole"

che consentono la re-installazione automatica

Problemi con Spyware

- **Tutta l'attività del browser può essere tracciata e monitorata**
- **Informazioni personali possono essere trasmesse o vendute a terze parti senza consenso e in modo del tutto inconsapevole**
- **Alcuni siti, senza autorizzazione, sono in grado di aggiungersi al desktop, all'elenco dei siti preferiti, o addirittura sostituirsi alla homepage (*hijacking*)**

- **Questi componenti malevoli non solo mettono a repentaglio la privacy, ma la stessa integrità del computer, oltre a diminuire l'efficienza (occupano spazio disco, memoria e rallentano le prestazioni)**
- **Attenzione particolare al furto d'identità virtuale**

Come accorgersi di avere uno spyware

Diversi sintomi possibili

- **Si vedono pop-up pubblicitari che appaiono sullo schermo, anche quando non si sta navigando**
- **La home page del browser o altre opzioni sono state modificate senza consenso**
- **Si nota una nuova toolbar nel browser che non è stata installata esplicitamente e che non si riesce ad eliminare**
- **Il computer impiega più del necessario ad eseguire alcune operazioni durante la navigazione**
- **Si sperimentano improvvisi crash del computer (es., blocco della tastiera o riavvio inaspettato del computer o di qualche applicazione)**

Difese

- **Installare ed eseguire uno dei seguenti prodotti *anti-spyware***

Spybot Search and Destroy
http://spybot.eon.net.au/index.php?lang=en&page=start

Ad-Aware (da Lavasoft)**
http://www.lavasoftusa.com/software/adaware/

****Gratuito per uso personale**

Modulo 3:
Firewall

Fondamenti comunicazioni Internet

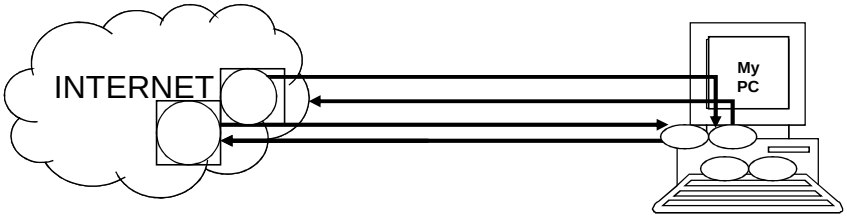
- **La comunicazione via Internet si ottiene mediante lo *scambio di molteplici "pacchetti" di dati***

- **Ogni pacchetto è trasmesso dal computer mittente al computer destinatario**
- **La "connessione" è in realtà costituita da singoli pacchetti che viaggiano tra due processi in esecuzione su questi due computer connessi ad Internet**
- **Ciascuno dei due computer (mittente e destinatario) inviano "pacchetti dati" e "pacchetti di servizio" ("ack") che indicano al la corretta ricezione dei "pacchetti dati"**

Comunicazione tra processi

La comunicazione è tra i processi in esecuzione su Computer, quindi viene identificata dalla quadrupla:

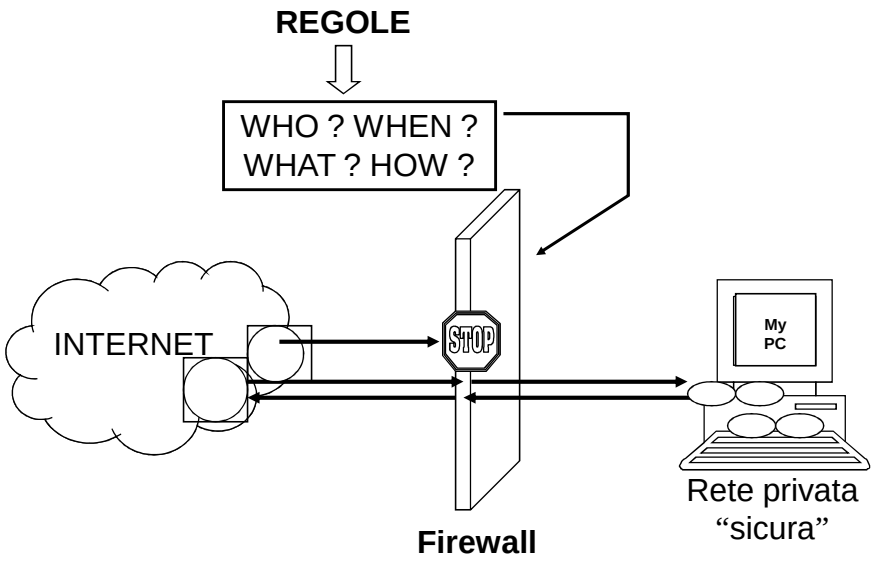
- **indirizzo IP mittente**
- **indirizzo IP destinatario**
- **porta mittente**
- **porta destinatario**



Cos'è un firewall?

- **Un sistema di sicurezza (software o hardware+software) che agisce come una fascia protettiva tra un computer (o una rete locale) ed il mondo esterno di Internet**
- **Isola il computer da Internet utilizzando un "muro di codice"**
  - **Ispeziona ciascun "pacchetto" in arrivo dall'esterno**
  - **Determina se lasciarlo passare o bloccarlo**

Come funziona



Compiti di un firewall

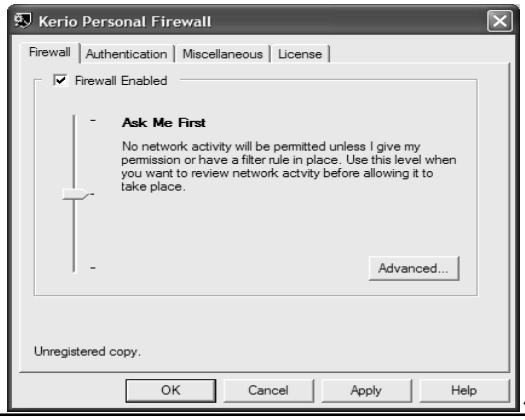
- **Il firewall è un software che ispeziona ciascun pacchetto non appena arriva alla macchina – PRIMA che il pacchetto venga trasmesso al processo che è in esecuzione sul computer**
- **Il firewall ha potere di veto totale su tutto ciò che il computer riceve da Internet**
- **Una "porta" TCP/IP è rilevata come "aperta" sul computer solo se il primo pacchetto del mittente che chiede una connessione, riceve una risposta dal computer destinatario**
- **Se, invece, la "porta è chiusa", il pacchetto in arrivo viene semplicemente ignorato e scomparirà da Internet. Significa che non è possibile utilizzare quel servizio Internet sul tuo computer**
  - *Evita di segnalare delle backdoor aperte!*

Efficacia del firewall

- **Il vero potere di un firewall è strettamente collegato alla sua capacità di selezionare COSA LASCIAR PASSARE e COSA BLOCCARE**
- **Un firewall può "filtrare" i pacchetti in arrivo sulla base di varie informazioni e decidere di bloccare o trasmettere i pacchetti**
  - Es: una qualsiasi combinazione di indirizzo IP della macchina mittente, della porta mittente e dell'indirizzo e della porta della macchina destinazione

KERIO firewall

- **Software o hardware tra la tua LAN e Internet, che ispeziona il traffico entrante sulla base di regole che possono essere stabilite dall'utente e che determinano il livello di sicurezza voluto**
- **Scelte di Kerio**
  - Permit Unknown
  - Ask Me First
  - Deny Unknown



Modulo 4:
Antivirus

Componenti di un antivirus

Con il termine antivirus in realtà si intendono più componenti differenti:

- **il binario in grado di ricercare il virus all'interno dell'elaboratore: è l'antivirus vero e proprio**
- **il binario che rimane residente e richiama l'antivirus ogni qual volta viene creato/modificato un nuovo file o una zona di memoria per controllare che il computer non sia stato infettato con tale operazione**
- **il file (o i file) delle firme: file che contiene tutte le *firme* dei virus conosciuti: è fondamentale ed essenziale per il funzionamento corretto di qualsiasi altro componente**
- **il binario che effettua gli update del file delle firme e di tutti i binari dell'antivirus**

Funzionalità

- **Le funzionalità che possono essere rinvenute in un prodotto antivirus si possono suddividere in due gruppi distinti**
  - Nel primo gruppo comprendiamo **le funzionalità di base**, orientate all'efficacia e all'affidabilità della protezione del computer
  - Nel secondo gruppo comprendiamo **funzionalità che possiamo considerare avanzate**, poiché facilitano l'utilizzo del prodotto od il suo aggiornamento

Funzionalità di base

- **Scansione in tempo reale di memoria e file**
- **Scansione degli allegati di posta elettronica**
- **Capacità di individuazione di varie tipologie di codice nocivo (cavalli di troia, backdoor, etc.)**
- **Verifica della integrità del settore di boot, del Master Boot Record (MBR) e dei file di sistema durante la fase iniziale di avvio del sistema**
- **Possibilità di creare dischetti di emergenza da utilizzare in caso di ripristino del sistema**
- **Rilascio da parte del produttore di frequenti aggiornamenti del file delle firme**

Funzionalità avanzate

- **Possibilità di programmare scansioni del file system ad intervalli regolari**
- **Possibilità di effettuare gli aggiornamenti attraverso Internet**
- **Capacità di isolare i file infetti per i quali il prodotto non sia in grado di compiere operazioni di pulizia**
- **Presenza di una guida esauriente che descriva le tipologie note di virus, cavalli di troia e backdoor e le loro caratteristiche principali**

Limiti dell’antivirus

- **L'antivirus è in grado di eliminare soltanto i virus che riconosce (presenti nel file delle firme)**
  - Tutti i nuovi virus possono passare completamente inosservati e fare tutto quello che vogliono senza che l'antivirus intervenga
- **L'antivirus può intercettare il virus solo quando questo è entrato all'interno del computer e quindi ha già infettato un file o la memoria**
- **Non sempre riesce a "disinfettare" il file o la memoria eliminando completamente il virus: in alcuni casi è costretto a mettere in "quarantena" il file contagiato ed eliminarlo per l'impossibilità di recuperare il file originario**

Limiti dell’antivirus

- **L'antivirus è un grande utilizzatore delle risorse del computer:**
  - Se avviato in background ogni volta che viene acceso il computer può comportare un forte rallentamento soprattutto nelle fasi iniziali
  - Possibile settarlo in modo da evitare la scansione dei file a seguito del boot

I nuovi virus

- **Antivirus diversi possono riuscire a rintracciare e controllare i nuovi virus prima di altri → importante la scelta**
- **La scoperta di un nuovo virus dipende anche da quanto è "infettivo“: più un virus si propaga velocemente e più è semplice individuarlo e aggiornare i file delle firme**
- **Può capitare che un antivirus consideri dei file o programmi come virali anche se in realtà non lo sono (falsi positivi)**

Falsi positivi

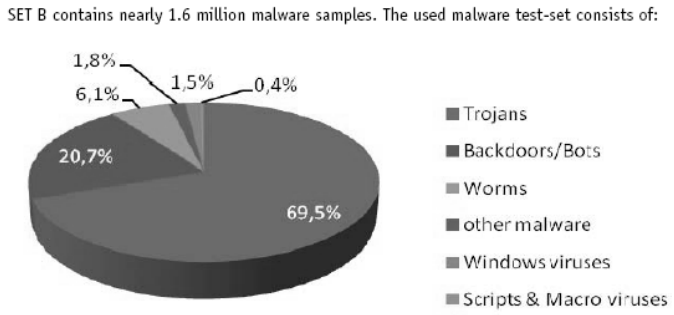
Cause dei falsi positivi

- **Un insieme di istruzioni che compongono un virus (od una sua parte) può essere presente anche in programmi e file "normali”**

Problema principale: si può non riuscire ad eseguire questo programma od aprire il file rilevato come infetto se prima non si disabilita l'antivirus, sempre che l'antivirus non lo abbia cancellato o rovinato in modo irreparabile nel frattempo cercando di proteggere il sistema

Comparativa

- **Test di diversi antivirus condotto da Independent Test of Antivirus software**
- **Set utilizzato: SetB contiene campioni di 1.6 milioni di malware scoperti negli ultimi 7 mesi**



Criteri di valutazione

- **Detection Rate**: Percentuale di malware rilevati
- **Falsi Positivi**: numero di falsi positivi avvenuti durante il controllo
  → da considerare insieme!!

	Detection Rates			
	<87%	87 - 93%	93 - 97%	97 - 100%
Few (0-15 FP's)	tested	STANDARD	ADVANCED	ADVANCED+
Many (16-100 FP's)	tested	tested	STANDARD	ADVANCED

Detection Rate

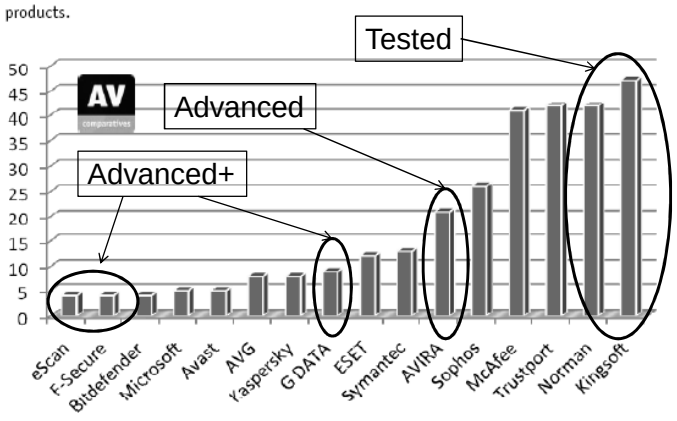
Total detection rates[2]:

1.	G DATA	99.8%
2.	AVIRA	99.4%
3.	McAfee[3]	98.7%
4.	Symantec	98.4%
5.	Avast	98.0%
6.	F-Secure	97.9%
7.	Bitdefender	97.8%
8.	eScan	97.7%
9.	Trustport	97.6%
10.	ESET	97.2%
11.	Kaspersky	94.7%
12.	AVG	94.0%
13.	Sophos	91.3%
14.	Microsoft	90.0%
15.	Kingsoft	86.4%
16.	Norman	84.8%

Nota: Symantec è Norton

Falsi positivi

The graph below shows the number of false alarms found in our set of clean files by the tested Anti-Virus products.



Scanning speed test

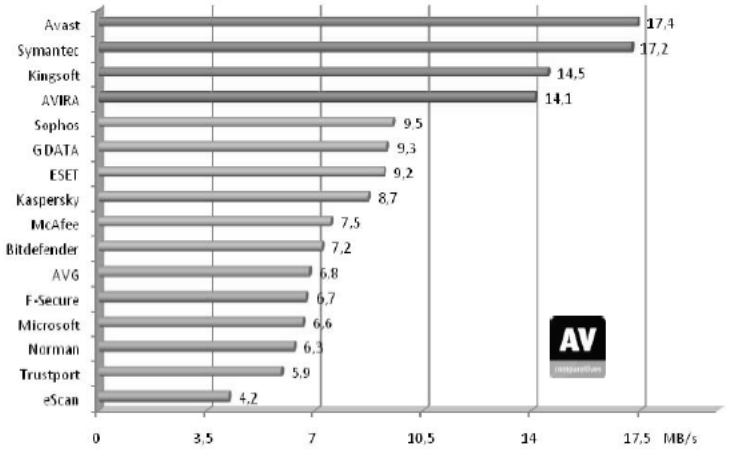
Modalità di scansione possibili

- **Short performance-optimzed scan**
  - Salta file già scansionati e non li ricontrolla
- **Full-security scan**
  - Ricontrolla sempre ogni file

Necessità di maggiore trasparenza nei confronti dell'utente circa la possibilità di attivare una o l'altra di queste modalità

Speed test

- **Throughput rate (MB/s) degli antivirus**



Classifica finale

Advanced+	G DATA Symantec Avast F-Secure BitDefender eScan ESET
Advanced	AVIRA* McAfee* TrustPort* Kaspersky AVG
Standard	Microsoft
Tested	Sophos* Kingsoft Norman

(*) Prodotti declassificati a causa dell'alto numero di falsi positivi

Consigli di base - riassunto

1. **Usare protezione di un software anti-virus**
2. **Aggiornare frequentemente anti-virus e sistema operativo ("patches" di sicurezza)**
3. **Non aprire allegati di email inattese o inviate da sconosciuti**
4. **Usare password difficili da indovinare**
5. **Proteggere il proprio computer da intrusioni via Internet – usare firewall**
6. **Fare back-up periodici dei dati sul computer**