Ulteriori Conoscenze di Informatica elementi di Statistica

Dr Carlo Meneghini
Dip. di Fisica "E. Amaldi"
via della Vasca Navale 84
st. – 83 – I piano
meneghini@fis.uniroma3.it
tel.: 06 55177217

http://www.fis.uniroma3.it/~meneghini

Sicurezza, amministrazione e manutenzione del sistema

- Virus: cosa sono, cosa fanno, come trattarli
- Malware: oltre i virus
- Antivirus e Firewall
- aggiornamenti e test di sicurezza
- configurazione del sistema (Windows)

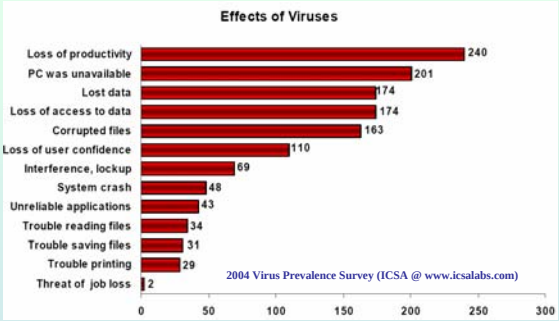
I virus

it.wikipedia.org/wiki/virus + informatica

Un virus codice in grado di infettare un programma ospite tramite il quale replicarsi e propagarsi ad altri programmi / sistemi con lo scopo di provocare danni / malfunzionamenti / effetti fastidiosi nel sistema quali:

- Visualizzare messaggi o effetti video.
- Cancellare files o formattare unità a 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

NOTA: un virus informatico, analogamente ai virus biologici, necessita di un programma ospite per operare. Con il termine Virus vengono spesso indicati altri tipi di malware quali worms, dialer, spyware etc...



Storia

Ipotizzati fin dagli anni 70 (fantascienza) il primo virus compare nel 1982: "Elk Cloner". Si propagava scambiando i floppy disk infettando il boot sector del sistema DOS 3.3 dei PC AppleII provocando effetti grafici, testo lampeggiante e la poesia:

ELK CLONER:
THE PROGRAM WITH A PERSONALITY
IT WILL GET ON ALL YOUR DISKS
IT WILL INFILTRATE YOUR CHIPS
YES, IT'S CLONER
IT WILL STICK TO YOU LIKE GLUE
IT WILL MODIFY RAM, TOO
SEND IN THE CLONER!

Tipi di virus

- Boot sector viruses: infettano i settori di avvio dei dischi
- Email viruses: si propagano via e-mail
- Logic bombs & time bombs: virus dormienti che si attivano quando si verificano date condizioni o ad una data specifica
- Macro viruses sono scritti come macro di programmi (tipicamente office) e infettano le applicazioni quali Word, Excel, Access etc...

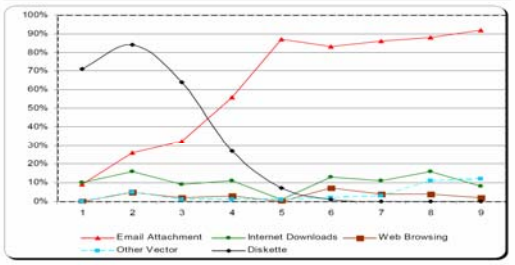
due tipi di malware spesso classificati come virus sono i

- Trojan horses (cavalli di Troia)
- Worms (vermi)

(vedi in dopo)

Metodi di propagazione

Virus Source	1996	1997	1998	1999	2000	2001	2002	2003	2004
Email Attachment	9%	26%	32%	56%	87%	83%	86%	88%	92%
Internet Downloads	10%	16%	9%	11%	1%	13%	11%	16%	8%
Web Browsing	0%	5%	2%	3%	0%	7%	4%	4%	2%
Other Vector	0%	5%	1%	1%	1%	2%	3%	11%	12%
Software Distribution	0%	3%	3%	0%	1%	2%	0%	0%	0%
Diskette	71%	84%	64%	27%	7%	1%	0%	0%	0%



2004 Virus Prevalence Survey (ICSA @ www.icsalabs.com)

Propagazione e tipi di virus

Per permettere ad unvirus di agire e replicarsi bisogna eseguirne il codice e scrivere nella memoria del PC. I virus propriamente detti si istallano in sezioni di programmi regolari e si attivano all'esecuzione del programma.

Si possono distinguere tra **virus non residenti**: cercano ospiti da infettare, li infettano e ne prendono il controllo. E **virus residenti**: non cercano un ospite ma si istallano nella memoria, rimangono attivi in background e infettano i vari programmi che vengono via via eseguiti

Ospiti (target)

- eseguibili: .exe, .com, .elf (Linux)
- volume boot records (VBR) e master boot record (MBR)
- script files di sistema quali .bat, VBscript, shell script (Unix/linux)
- script e macro file di applicazioni specifiche (word, excel, Access, outlook, etc...)

Molti virus contengono codici di cifratura e mutazione per renderne difficile il riconoscimento. Si parla di virus polimorfici e matamorfici

Danni provocati da un virus

Win.CIH non si limita a sovrascrivere i dati sul disco rigido, ma riesce anche a modificare il contenuto della memoria Flash su cui è memorizzato il Bios rendendo impossibile l'avviamento del sistema.

W32.Netsky.X@mm è una variante di W32.Netsky.W@mm: esegue una scansione di tutte le unità, escluse quelle CD-ROM, sul computer infetto alla ricerca di indirizzi e-mail. Utilizza quindi il proprio motore SMTP per inviarsi a tutti gli indirizzi di posta elettronica che trova. Il mittente del messaggio di e-mail è mascherato e l'oggetto, il corpo del messaggio e l'allegato variano. L'allegato ha l'estensione .pif.

Database e informazioni

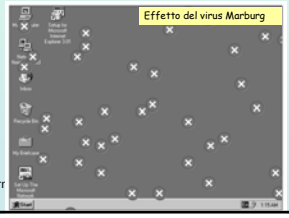
www.viruslibrary.com,

www.viruslist.com

www.icsalabs.com

www.symantec.com

www.wildlist.org



Difesa dai virus

- Effettuare regolarmente il backup dei dati.
- Tenere gli antivirus aggiornati (settimanale/giornaliero)
- Aggiornare regolarmente il sistema operativo e i programmi.
- Preparare un disco di emergenza.
- Non aprire mai distrattamente un allegato di posta elettronica.
- Non eseguire mai un programma di fonte incerta.
- Non eseguire mai macro sconosciute di un documento di Office
- (www.punto-informatico.it, www.symantec.com,

Tenersi informati sulle caratteristiche nuovi virus

- www.punti-informatico.it,
- www.symantec.com,
- www.wildlist.org
- www.hoax-slayer.com

Effetti del w32.netsky e removal tool

In caso di infezione

- Non scambiare file con altri utenti.
- Non continuare a lavorare con la macchina infetta
- Cerca informazioni su Internet: (www.symantec.com). Si possono trovare sul WEB le procedure e le utility per rimuovere il virus e (forse) recuperare i dati danneggiati.
- Ripristina la funzionalità del computer.

In caso di sospetta infezione è utile eseguire lo scan del PC utilizzando windows in modalità provvisoria (tasto F8 all'avvio) e utilizzando utility di scansione on-line

Security Check for Home Users, che puoi trovare sulla home page di Symantec (www.symantec.it).

Panda Software, www.pandasoftware.com e fare clic sulla zona **Panda ActiveScan**.

Trend Micro offre il servizio, **HouseCall**, raggiungibile alla pagina Web housecall.antivirus.com.

Worms e Trojan

Un **worm**, come un virus, è un malware in grado di diffondersi, autoreplicarsi e causare danni ma, a differenza di un virus non necessita di un programma ospite per funzionare. Utilizza la rete internet per propagarsi. Di solito influenza le prestazioni di connessione in rete.

Prendono il nome da un "virus" descritto in un romanzo di fantascienza (*The Shockwave Rider*, J. Brunner - 1975) in grado di propagarsi in una rete di computers. I primi worms compaiono intorno alla fine degli anni 80 (~1988)

Tipi di Worms

e-mail worms: si propagano attraverso la posta elettronica. Il worm i replica e si autoinvia a liste di corrispondenti vie e-mail fasulle mascherando il mittente.

Instant messaging worms: si diffonde usando i messagi istantanei (es.: windows messenger) fornendo link a siti infetti.

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

File sharing network worms: si istallano nelle directories condivise con nomi innocui

Internet Worms: usano protocolli di basso livello (TCP/IP) per propagarsi. Spesso utilizzando vulnerabilità specifiche del sistema.

Effetti

Molto spesso un worm è fatto per disturbare le comunicazioni via rete occupando la banda. Tuttavia un worm può contentere codici per danneggiare il sistema ospite, cancellare i files o diffondere informazioni sensibili. Un azione tipica del worm è quella di aprire una connessione (backdoor) sul PC infetto che consente ad altri di utilizzarlo via rete. Si parla di Zombie computer: PC la cui sicurezza è stata compromessa e sotto il controllo di altri Sobig & Mydoom sono tipici esempi di worms di questo tipo.

I worms si diffondono soprattutto utilizzando vulnerabilità dei sistemi operativi o ingannando gli utenti. Per limitare i rischi di infezione è fondamentale istallare gli aggiornamenti di sicurezza.

W32.Sobig.F@mm

* Damage Level: Medium

* Large Scale E-mailing: Sends email to addresses collected from files with the following extensions: .wab, .dbx, .htm, .html, .eml, .txt.

* Releases Confidential Info: May steal system information, including passwords.

14

W32.Mydoom.AS@mm

Discovered: February 9, 2005
Updated: March 15, 2005 10:32:25 AM PST
Also Known As: Win32.Mydoom.AP [Computer Associates], Email-Worm.Win32.Mydoom.ak [Kaspersky Lab], W32/Mydoom.ba@MM [McAfee], W32/MyDoom-AR [Sophos], WORM_MYDOOM.AR [Trend Micro]
Type: Worm
Infection Length: 33,792 bytes
Systems Affected: Windows 2000, Windows 95, Windows 98, Windows Me, Windows NT, Windows Server 2003, Windows XP

W32.Mydoom.AS@mm is a mass-mailing worm that uses its own SMTP engine to send itself to email addresses that it finds on the compromised computer. It also propagates through file sharing networks.

The email will have a variable subject and attachment name. The attachment will have a .bat, .cmd, .exe, .pif, .scr, or .zip file extension.

Damage
* Damage Level: Medium
* Large Scale E-mailing: Sends itself to email addresses gathered from the compromised computer.
* Modifies Files: Modifies the hosts file.
* Compromises Security Settings: Disables antivirus and firewall applications, blocks access to security-related Web sites.

Distribution
* Distribution Level: High
* Subject of Email: Varies
* Name of Attachment: Varies with a .bat, .cmd, .exe, .pif, .scr, or .zip file extension

Trojan

Un cavallo di Troia (trojan horse) è un malware che deve il suo nome al fatto di essere celato all'interno di un programma apparentemente utile. Sono ampiamente utilizzati per inviare spam, registrare dati personali (password e numeri di carte di credito), danneggiare files. A differenza di un virus i trojan non si auto-replicano.

On the Microsoft Windows platform, an attacker might attach a Trojan horse with an innocent-looking filename to an email message which entices the recipient into opening the file. The Trojan horse itself would typically be a Windows executable program file, and thus must have an executable filename extension such as .exe, .com, .scr, .bat, or .pif. Since Windows is configured by default to hide filename extensions from a user, the Trojan horse is an extension that might be "masked" by giving it a name such as 'Readme.txt.exe'. With file extensions hidden, the user would only see 'Readme.txt' and could mistake it for a harmless text file. Icons can also be chosen to imitate the icon associated with a different and benign program, or file type, and (types)

When the recipient double-clicks on the attachment, the Trojan horse might superficially do what the user expects it to do (open a text file, for example), so as to keep the victim unaware of its real, concealed, objectives. Meanwhile, it might discreetly modify or delete files, change the configuration of the computer, or even use the computer as a base from which to attack local or other networks - possibly joining many other similarly infected computers as part of a distributed denial-of-service attack (zombie PC)

A destructive program that masquerades as a benign application. Unlike viruses, Trojan horses do not replicate themselves but they can be just as destructive.

en.wikipedia.org

Tipi di Trojan horses

Remote Access Trojans
Data Sending Trojans
Destructive Trojans
Proxy Trojans
FTP Trojans
security software disabler Trojans
denial-of-service attack (DoS) Trojans
URL Trojans

Effetti

cancellazione dei dati.
criptare i files a scopo di ricatto.
danneggiare i files.
mandare e ricevere files.
registrazione di screenshots.
registrazione diinformazioni di login
registrazione di dati bancari
istallazione di backdoor su un PC.
raccolta di indirizzari e spamming.
permettere l'accesso remopto ad altri (RAT-remote administration tool)
favorire la diffusione di virus e malvare (vettore o untore)
creare network di computer zombie per spamming e attivita' illecite.

en.wikipedia.org/wiki/Spyware

Spyware

Uno spyware è un programma che raccoglie in modo subdolo informazioni personali dell'utente. Termine coniato intorno al '95 e rapidamente diffuso dopo il 2000. Uno spyware utilizza tecniche subdole quali il keylogging (registrazione dell'attività sulla tastiera), la registrazione dell'attività di surfing, analisi dei documenti sull'HD, etc... al fine di carpire informazioni

Possono registrare e inviare ad altri dati sensibili o semplicemente registrare le abitudini dell'utente per consentire una pubblicità mirata. Spyware sono spesso istallati insieme a programmi shareware e multimediaali

Adware

Deriva da advertising (advertising-supported software) e si riferisce a programmi pubblicitari, spesso senza il consenso dell'utente. Eudora invia messaggi pubblicitari per la versione free.

Tracking

Alcuni adware fanno uso di codici che registrano l'attività in rete (tracking cookies) per tracciare un profilo utente e sottomettere pubblicità mirata.

Protezione da Spy e Ad

Diffidare di freeware e shareware: informarsi prima di istallare un software dichiarato freeware, shareware, gratuito etc... Nota: La maggiore espansione di virus su sistemi microsoft non è dovuta, alla maggiore vulnerabilità del sistema windows ma deve essere attribuita alla minore esperienza e maggiore ingenuità dell'utente medio windows (nel 2005 di circa 5000 vulnerabilità meno di 1000 sono state osservate su sistemi microsoft, circa 2000 su SO unix/Linux e circa 2000 multipiattaforma).

utilizzare un firewall
Kerio Personal Firewall (30day full free dopo free con alcune limitazioni)
www.sunbelt-software.com/Kerio.cfm

istallare un filtro anti-spy e Ad-remover
spybot search and destroy (www.spybot.info).
ad-aware (SE personal) (Lavasoft) (www.lavasoft.com)

Spam, Hoax & Phishing

La maggiore espansione di virus su sistemi microsoft non è dovuta, alla maggiore vulnerabilità del sistema windows ma deve essere attribuita alla minore esperienza e maggiore ingenuità dell'utente medio windows

Spam: comunicazioni non richieste e insistenti di prodotti anche illeciti e illegali. I messaggi Spam contengono spesso link a siti contente materiale pornografico, offensivo, illegale etc...

Il danno è principalmente nell'occupazione della capacità dei servers (fino a 1/3 delle mail di AOL è occupata da messaggi spam)

Lo spam si diffonde via mail in modo diretto o sfruttando l'ingenuità e buona fede degli utenti.

Catene di messaggi, inviti a diffondere notizie etc.. sono un mezzo per diffondere messaggi spam.

NON RISPONDERE ALLE MAIL SPAM rispondere ad un messaggio di spam indica allo spammer che l'account è attivo!

NON RIMANDARE IN MODO A-CRITICO AVVISI, ANNUNCI, APPELLI.

Gli Hoax (bufale/burle) sono informazioni false o artefatte con avvisi di virus disastrosi, malattie, richieste di auito, casi umanitari etc... che quasi mai risultano vere. Un elenco aggiornato (italiano) si può trovare su www.attivissimo.net/antibufala. Prima di inviare queste mail fare una rapida ricerca sulla rete per controllarne la veridicità

Il phishing è un'attività criminale tramite cui vengono acquisite informazioni sensibili (carte di credito, coordinate bancarie, password, etc...) mascherandosi da ente/società/persona di fiducia.

Il phishing avviene tramite e-mail o instant message. Spesso si danno link a siti web copia di siti accreditati (banche, enti etc...).

Alcuni di questi siti sono disabilitati in Explorer, Mozilla, Opera etc...

NON FORNIRE PER ALCUN MOTIVO DATI SENSIBILI (password, numeri CC, coordinate bancarie, etc...)

Antivirus

Un antivirus è un programma in grado di rilevare e rimuovere codici malware quali virus, worms, dialers, trojan.

Funzionamento:

1) ricerca in RAM e nei files del codice identificativo (firma) del virus.

2) controllo in tempo reale di files e programmi in transito (mail, WEB, download)

Il successo di questi programmi risiede nel continuo aggiornamento delle liste di firme dei virus conosciti (almeno settimanale, in caso di connessioni veloci è utile e poco dispendioso l'aggiornamento giornaliero)

Antivirus

Elementi di un AV:

1. il/i file delle firme
2. il codice in grado di cercare i virus nel PC
3. il codice che controlla i files in tempo reale
4. il codice per eseguire l'aggiornamento automatico delle liste

Un virus attivo (virus, trojan, etc...) può disattivare in toto o in parte l'antivirus.

Un antivirus può rimuovere i files infetti ma spesso è inefficiente contro i virus residenti per i quali è necessario uno strumento di rimozione opportuno e procedure a volte complesse

In caso di infezione può essere utile effettuare una scansione usando programmi esterni (via rete: es. trend-micro package)

AVAST (www.avast.com) è attualmente uno dei migliori antivirus freeware in circolazione

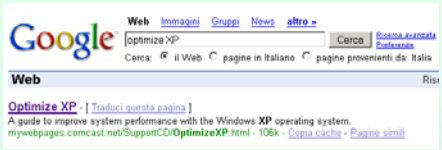
I firewall

Un firewall permette di controllare l'accesso al proprio PC, selezionare le applicazioni da eseguire, limitare l'accesso in base a regole opportune, etc..

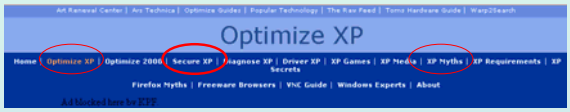
Kerio Personal Firewall

www.sunbelt-software.com/Kerio.cfm

è un ottimo firewall, gratuito per i primi 30 gg, poi vengono ridotte alcune potenzialità. Il vantaggio del KPF è un monitoraggio efficiente non solo delle comunicazioni ma anche di tutte le operazioni svolte dal PC: es. avverte se un'applicazione è stata modificata dall'ultimo utilizzo, avverte se un'applicazione avvia un processo indipendente etc... (comportamente tipici di malware). Controlla l'apertura di pop-up e l'attivazione di Adware da parte di pagine WEB.

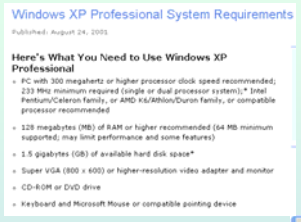


http://mywebpages.comcast.net/SupportCD/**OptimizeXP**.html



1) aggiornamento del SO

http://www.microsoft.com/windowsxp/pro/upgrading/sysreqs.mspx



Prima di agire sul SO effettuare un backup completo dei dati e delle impostazioni cruciali (rete, password, configurazioni di connessione). Controllate di avere i dischi originali e i codici di accesso.

Service Pack 2

Microsoft Windows XP Service Pack 2 (SP2) provides new proactive security technologies for Windows XP to better defend against viruses, worms, and hackers. In addition to a more robust security infrastructure, SP2 improves the security configuration options of Windows XP and provides better security information to help users faced with security decisions.

Aggiornamenti automatici

I service pack raccolgono tutta una collezione di upgrades. Tuttavia gli aggiornamenti sono prodotti costantemente. Quindi l'aggiornamento del sistema deve essere effettuato con regolarità.

> Start

> control panel

classic view → > system → > Automatic Updates

category view → > performance and maintenance → > system → > Automatic Updates

Pulizia da malware/spyware

CCleaner è un programma freeware che rimuove i file non utilizzati velocizzando Windows e liberando spazio disco.

Ad-aware è un software freeware per rimuovere Spyware, Adware, hijackers a altro malware

Spybot - Search and Destroy è un software freeware per rimuovere Spyware, Adware, hijackers a altro malware

Microsoft Windows Defender è un software freeware che aiuta a difendere il PC da danni dovuti a malware. Attenzione: Microsoft Windows Defender indica come spyware molti programmi Peer to Peer. Prima di rimuovere un'applicazione o altro assicurarsi di quello che si vuole fare (www.spywareguide.com)

Protezione dagli spyware

Diffidare di freeware e shareware: informarsi prima di istallare un software dichiarato freeware, shareware, gratuito etc.. Verificare sul sito: www.spywareguide.com

Spybot - Search and Destroy

Impedisce l'istallazione di spyware basati su applicazioni Active-X

Firewall

Windows XP firewall

(start > settings > firewall)

E' incluso nella distribuzione WXP e automaticamente attivo nella SP2. Manca un rapporto di attività, utile per utenti più esperti.

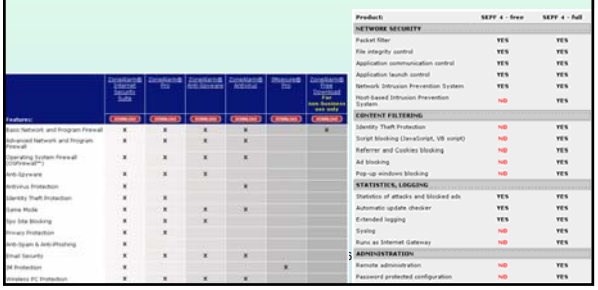
Zone Allarm è un ottimo Firewall, freeware per uso personale.

Nota: non utilizzare più di un firewall attivo per evitare competizioni dannose

Zone Allarm KPF sono freeware per uso personale.

Zone Allarm

Sunbelt Kerio Personal Firewal



Utilities (www.grc.com/unpnp/unpnp.htm)

Unplug n' Pray:

Disabilita il servizio Universal Plug and Play networking.

Il servizio Universal Plug & Play non è connesso con il sistema standard di Plug & Play dell'hardware.

DCOMbobulator

Il sistema DCOM (Distributed Component Object Model) permette di attivare in modo remoto componenti del vostro S.O. e di utilizzare sulla rete!!!

WXP SP2 non è vulnerabile

shoot the messenger

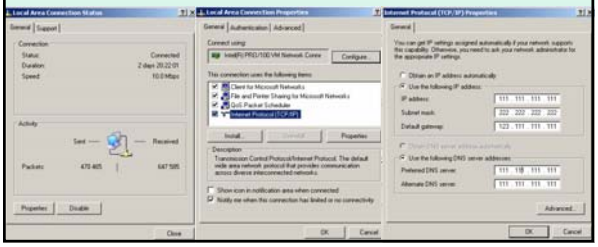
Il servizio "Messenger" è utilizzato per diffondere messaggi SPAM.

In WXP SP2 è (o dovrebbe essere) disabilitato.

Test di sicurezza

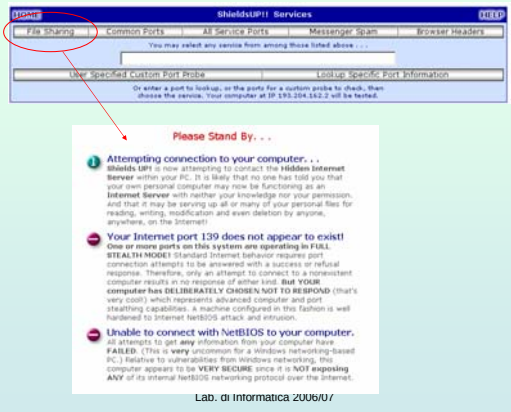
www.dshield.org/warning_explanation.php

Your IP (###.###.###.###) does not appear as an attacker in the DShield database.

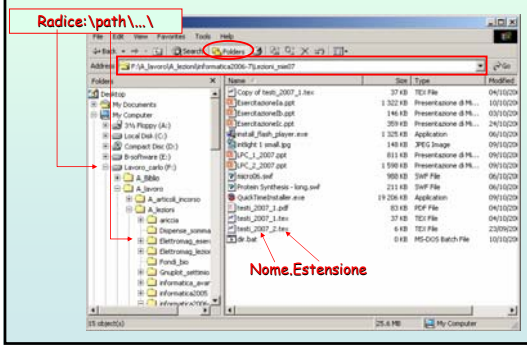


Check dello stato di sicurezza

GRC Shields Up

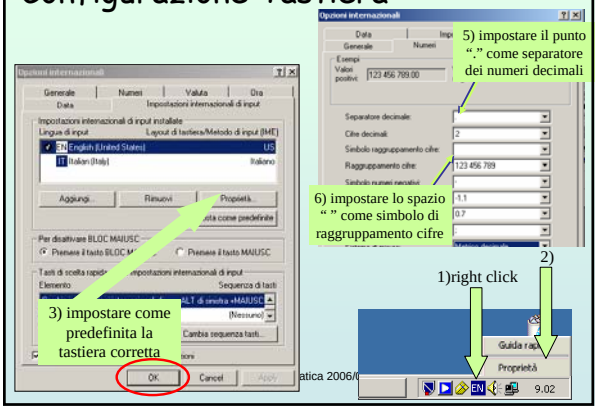


File System di windows (organizzazione dei files)

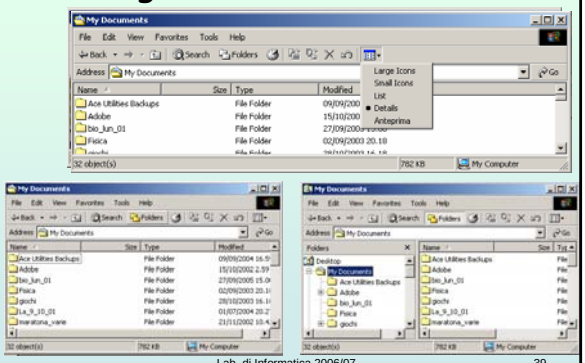


37

Configurazione Tastiera

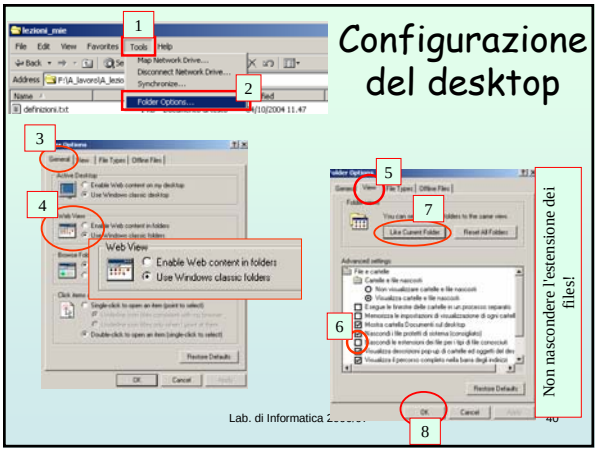


Configurazione delle cartelle



Lab. di Informatica 2006/07 39

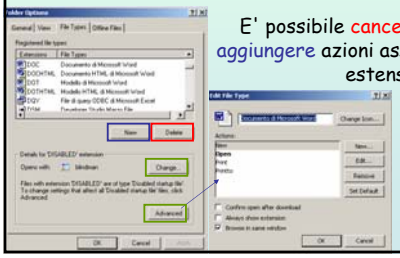
Configurazione del desktop



Lab. di Informatica 2006/07 40

Nota: estensioni

L'estensione permette all'utente e,a volte, al software, di distinguere tra i vari formati di file. Windows (ma non solo) associa automaticamente un'applicazione ed un azione ad una data estensione del file.
L'associacione estensione-formato è una convenzione non vincolante: l'estensione può essere modificata o rimossa senza perdere o modificare il contenuto e il formato del file stesso



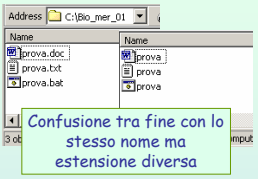
E' possibile cancellare, modificare aggiungere azioni associate ad una data estensione.

Da usare con cautela !

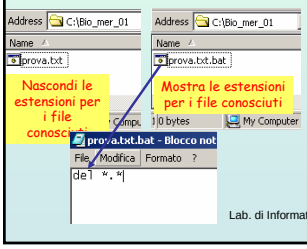
41

Problemi di sicurezza

L'impostazione predefinita di windows nasconde le estensioni dei files conosciuti.



Confusione tra fine con lo stesso nome ma estensione diversa



Il file:
prova.TXT.bat
che contiene macro e comandi potenzialmente pericolosi che vengono eseguiti automaticamente al click del mause, è visualizzato come:
prova.TXT
che somiglia ad un innocuo file di testo!

Ottimizzare le performaces

start
>settings
>system