Computer Viruses

INFO 100
Friday, December 7, 2001
Scott Barker

What is a Computer Virus?

- You tell me!

My definition

- A virus is something that propagates itself and causes damage, annoyance, or lost productivity
- We usually think of computer viruses as computer programs but that's not always so…
- Some viruses may just be text that propagates itself by asking humans to do something they shouldn't
  - Example: "Good times" virus
- Some don't consider these viruses but instead pranks or hoaxes. But the damage done or time wasted can be the same

More Precisely

- Programs like this are often placed into different categories depending on how they work.

  Hoax or Prank – a claim that something bad will happen to you under some circumstance (such as reading a message with "Good Times" in the subject) that is not true. You are asked to send email to all your friends to warn them.

  Trojan Horse - claims it is a program to do one thing but actually does something else

Traditional Virus

- A piece of computer code that is attached to an executable program.
- Typically this code works in such a way that the original program still runs as normal so that the end-user user does not know they were infected.
- This additional code may then do things malicious like delete files on your hard drive on a particular date, or it might do something that is just annoying like placing a popup message on your computer.
- Sometimes the virus will propagate by attaching itself to other executable programs as they run. So as you run more programs, the virus spreads

How do they get started?

- Think about the programs you have written. Could you easily create a virus like this or not?

  What do you think would have to be done to make a virus of this type work?

  – Need a starting place, an existing program that people are likely to run on their computer that you can infect

  – You then have to alter that program in such a way that your program will run first, then the real program will run after so that people don't know your program is active

  – This is hard

Think about what programs are…

Fundamentally, what is an executable program?

- A series of binary 1's and 0's – machine code. Once a program has been compiled, it isn't in a higher level language like Visual Basic or C that you can read and easily alter.
- So…you would have to write this virus code in some language, compile it into machine code, and then insert that new code into the original executable program that you want to infect
- Typically the first instruction of your program would be to jump to a new location to execute the code you have added, and then when your program is done running, jump back and start the old program as normal.
- Again, this is done so that people aren't aware that they are infected. If the regular program didn't work, they would be suspicious.

– After all that, you need a way to propagate this program.

– How might you do it so your virus could infect others?

Bottom line on Traditional Viruses…

- Not that common today
- Modern operating systems protect key system files from modification insuring that they cannot be infected
- Because they are hard to write, not lots of people have the skills necessary
- To be infected by a traditional virus you would have to run an executable program (.exe, .com)
- There are easier ways to wreak-havoc if that's your intention

Macro Viruses

- Probably the most wide spread virus type today
- What is a macro?
  - Simple program that is usually written inside another application such as Word or Excel
  - Macros have been around for years, in Word Perfect for DOS, Lotus 1-2-3
  - Many organizations/corporations use macros to automate routine operations
  - In Microsoft Office, macros are typically written in Visual Basic for Applications (VBA). Other apps have their own macro languages.
  - Macros are saved inside files, like Word documents or Excel spreadsheets
  - Word and Excel can be set to automatically run any Macros that are in a document or spreadsheet whenever one is found (and many years ago this was the default, but not today)

So what is a macro virus?

- Simple!
  - Again it is code that is designed to do something malicious, annoying, or to just waste your time
  - What distinguishes it from a regular virus is that it is much easier to write since an easy to use language is available (VBA) and…
  - It is easy to distribute since any old word processing document can contain the macro and…
  - It can easily and quickly propagate since people share and exchange document files much more frequently than they share and exchange executable programs

Bottom line on Macro Viruses

- Very common today
- To be infected you have to open a document or spreadsheet that has a macro in it and…
- Your application (like Word or Excel) has to then run the macro
- Today by default newer versions of Word or Excel will warn you if a document has a macro before it runs

Worms

- Worms are programs that are designed to search for known vulnerabilities and exploit them.
- They are typically able to propagate very quickly and are the source of most of the serious virus outbreaks that we hear about on the news
- Some are stand-alone programs that scan other computers on the network looking for known operating system security holes. Once they find a hole, they propagate by copying themselves to that new host. Once on the new host they scan for additional computers to infect.
- Others worms are in essence macro viruses that use known vulnerabilities in applications (like Outlook or Outlook Express) to propagate (using the Outlook Address book for example).
- Other worms may try and use code embedded in an HTML based email message (such as Java or JavaScript) again to exploit known vulnerabilities in applications like Outlook

Email Viruses

- Probably the most common source of virus infection today is email
- Why?
  - Email message attachments are how people today typically exchange files and documents.
  - As we said, executable files may have viruses attached to them, or documents may have macro viruses in them.
  - Many email programs today allow people to open attachments very easily (just double click the attachment name)

Why are attachments dangerous?

- If the attachment is an executable file, the program will run and you may be infected.
- If the attachment is a macro virus, it may open and run automatically if your word processing or spreadsheet application is not configured to block macros. Even if it is, and you are prompted – many people don't know to answer "no" and allow the macro to run anyway
- If the attachment is a worm, it may open your Outlook address book and email itself to all your friends and relatives

HTML Messages Also Dangerous

- Even if an email message doesn't have an attachment it is potentially dangerous as a program could be embedded in the HTML code.
- Some email programs like Outlook display HTML messages in a preview window so that code may execute as soon as you click on the message

The Case For and Against Outlook

- Many people complain that many of these problems are the fault of Microsoft and their email clients Outlook and Outlook Express.
- There are reasonable arguments to be made both ways.

Against Outlook and Windows

- Outlook and Windows in general does make it easy to open files. Double click an attachment name and the file opens.
- Outlook does allow HTML messages to be sent and displayed.
- For a long time macros were allowed to run by default in Word and Excel
- Microsoft does have an easy to use scripting language (VBA) that makes it relatively easy to write macro viruses
- Windows by default hides program extensions like .exe, so an end-user can be fooled into opening a file that they shouldn't
- If Microsoft wrote it, it must be bad and insecure
- The vast majority of viruses target Outlook and Outlook Express users. People that use other email programs do not have as many problems.

For Outlook

- Outlook and Outlook Express are far and away the most popular email programs. If you were writing a virus and wanted to make an impact, you wouldn't target a program that has very few users. If everyone switched to something else, the virus writers would change too.
- One of the reasons Outlook is so popular is ease of use. On Unix Pine for example you have numerous steps you have to carry out to open or send an attachment. As a result people rarely used attachments with that application, hence it isn't as big a problem.
- Microsoft has changed the default behavior of applications like Word and Excel to prevent macro viruses from running automatically.
- For almost two years, Microsoft has had patches to Outlook and Outlook Express that prevent certain file types (like .exe's) from running if you just double click on an attachment.
- Similarly Microsoft has released patches to prevent other programs from automatically opening your address book and sending email to others. Yet users and system administrators have not installed these fixes – some electing to skip them because it is inconvenient. Many times end-user pick ease of use over security. What do you think?

What can you do about Viruses?

- Remember:
  - Exchanging files can be dangerous
  - Where did the file come from, could it be an executable program or could it contain a macro virus?
    - Suggestion: Turn on file extensions in Windows so you know for sure
  - In an email message, is this message really from the person that it claims to be from or could it have been automatically generated?
    - Suggestion: If you aren't sure, send them a message and ask. Treat messages with unusual subjects or messages that ask you to click a link or do something specific on your machine VERY suspiciously

More suggestions

- Is there an attachment on this message and if so, do I really want to open it?
  - Again look at the file extension. Who sent you this attachment, are they sending you an enticing message that makes you want to look? If so, be suspicious.
- Is my machine updated with the latest operating system patches so that it can't be exploited by worms?
  - Suggestion: On Windows machines run Windows update frequently and install the fixes
- Are my applications up to date and do I have the security patches installed for my email program?
  - Suggestion: Try and always use the most latest version and checkout the email vendor's site occasionally to make sure you have the latest security patches installed. Consider turning off the message preview feature in Outlook.

Anti-Virus Products

- Consider installing an anti-virus program on your computer. McAfee and Norton are a couple of the more popular. McAfee's Virus Scan is available as part of the UWICK kit or can be downloaded from:

www.washington.edu/computing/software/sitelicenses/virusscan

How do virus scanning programs work?

- Basically they look for "signatures"
  - A signature might be the binary code that is added to an executable file when it is infect. This code would be unique for each virus.
  - The signature might also be some text that is in the contents of a macro
  - Or the signature might just be a file name that is known to be a virus
- Some virus scanners check all your files as they are opened, some scan files "on demand", others may just scan incoming email attachments
- Remember though, new viruses are released all the time – so in order to be effective a virus scanning program must be updated all the time as well
  - Just having a virus scanner running on your machine doesn't protect you. It's only as good as the last time it was updated. And…if a brand new virus comes out you could get infected before the vendor of the software has even had time to come out with a signature that looks for that virus

Why do we have Viruses?

- Like everything else in society, some people are malicious
- Others are looking for fame or attention
- Others enjoy a challenge and find the idea of causing massive disturbances to be exciting
- Some have personal grievances, for instance they don't like Microsoft so they decide to target their products for attack hoping people will switch to something else
- Some may just want to make a political statement for instance the "Hacked by Chinese" worm that went out slightly after an America plane had an incident with a Chinese pilot

The Threat

- We have already seen that viruses and worms can have significant effects on business, industry, and government
- Given today's political climate viruses and worms are a significant concern
- Sometimes though, people get too carried away and go to ridiculous extremes like refusing to ever use attachments in email, or only using some obscure email client so they won't subject to any attack on Microsoft software.
- Others blame every little system problem possible on viruses, when that usually is not the case.

Conclusion

- Be aware of the damage that viruses can do
- Take reasonable precautions to protect yourself
- Use good judgment when exchanging files, downloading files from the Internet, or opening attachments
- Install a virus scanner on your machine and keep it updated
- Don't propagate viruses hoaxes to others. Unless you are REALLY sure that something is a virus and you REALLY are sure you need to warn others don't.
- Remember that many viruses using social factors to try and get you to run them. They say they are from a friend, or they tell you someone loves you, or they say there is a sexy picture to look at. Don't be fooled.
- Don't go overboard and don't worry excessively about them. The vast majority of viruses can be cleaned from your system fairly easily, and most do relatively little damage. Be smart, not paranoid!