Worms, Viruses and Other Icky Stuff

Al Williams (alw@psu.edu)
Penn State Teaching and Learning with Technology
SHARE 98, Nashville, TN
Session 5820
My Group

- Classroom and Lab Computing (name changed from Distributed Computing)
  - About 30 full time & 60 hourly employees
  - Student Labs (44)
  - Technology Classrooms (126)
  - Workstations and Servers (2000)
  - Serve up applications (hundreds)
  - 42K Students at University Park campus
  - 80K Students system-wide
Topics of Discussion

- What Are We Dealing With
- Locked Down and Safe?
- Historical Perspective
- Things That Hurt
- Current efforts
- Lessons Learned
- What next?
What’s a Virus

- **THE NECESSARY CONDITION OF BEING CONSIDERED A COMPUTER VIRUS** is the capability to produce copies of itself (not exact bytewise replicas) and to incorporate them into computer networks and/or files, system areas of computers, and other executable objects. In addition to that copies also maintain the capability to spread further.
Worms

- These programs spread in a computer network and, like viruses-"companions", don't change files or sectors on disks. They penetrate the computer's memory from a computer network, calculate network addresses of other computers and send their own copies to these addresses.
Trojan Horses

• This is a program or part of program code that performs destructive actions, i.e. depending on some conditions wipes out information on disks, hangs the system etc.
Other Icky Things

- Denial of Service
- Combinations
- Smart Viruses
- Zombies
- Macro viruses
Historical Perspective

• Does it seem like we are getting attacked more often?
• Does it seem like we are getting more different kinds of attacks?
• YES!
Review of Advisories

• CERT Windows focused advisories
  – 1999 there were 4
  – 2000 there were 8
  – 2001 there were 14
  – Have 2 already for 2002

• For full picture see
  – http://www.cert.org/stats
  – http://www.cert.org/advisories
Locked Down Implies Safe?

• Student machines
  – Restrict write access
  – Prevent boot of other media
  – Administrative password
  – Refresh initialization files
  – Physical security

• Run Virus software here
  – Not at first
  – MacAfee last year
  – Norton Antivirus now
Locked Down Servers

- Tight ACLs
- Strong passwords for admin privileges
- Physical security
- Limited number of people who are authorized to make changes
- Did not run Virus Scans here
  - Concerned about performance & privacy
But Wait!

- Student space on central file server
  - Students manage own ACLs
- Instructor shares on central servers
  - Instructors manage own ACLs
- Student media
- Student and instructor private machines
Still Vulnerable

• Access to file servers by students and faculty from their machines
• Open permissions on shares set by students or faculty
• Server deployed applications that write back to their own directories
  – “ill formed applications”
• FTP servers to faculty shares
Guilty by Association

- Data on our servers can get contaminated
- Ill formed applications become victims and even spread viruses
- Enabling shared data helps spread viruses
- Providing remote access is a good service but
  - At the mercy of how others manage their computers
Some Incidents That Hurt
Melissa

• MS Word macro virus
• Replaces normal.dot
• Anything you save becomes template
• Sends infected documents to others in your address book
Melissa Cure

• Maintenance on Office
  – Warns about imbedded macros
• Delete normal.dot
• Run virus scanning software
Smurf Attack

- a.k.a. Tribe Flood
- Virus plants Trojan horse
- Trojan horse phones home
  - Awaits command
  - On command sends specific string to targets
  - Could be ping with spoofed origin
  - Could be mal-formed packet that crashes your system
Smurf Cure

- Don’t route packets with spoofed source
- Don’t route broadcast packets
- Work with security team to locate infected machines and repair
- Grit your teeth and endure…
- Worst case – sever connection to Internet
Smurf Exposures

- Centrally managed routers tend to be OK
- Privately managed routers not
  - Software router on NT server
  - Personal and departmental routers
- Even had this in my labs
  - Mac Ethernet routed off Windows Token Ring
VBS Worm

- Annakarnakova.jpg.vbs
- Attachment is VBS script (masquerading as a jpeg)
- Email invites you to look at the picture
- Bad settings in Outlook Express or Outlook automatically execute .vbs
- Hidden file extension only shows Annakarnakova.jpg
- Wipes out all your jpegs
- Sends itself on using your address book
VBS Worm Cure

• Maintenance from Microsoft to lock down Outlook and Express
• Don’t open that attachment!
• Tough luck if you didn’t have a backup
  – Your Jpegs were gone
• Virus scanners catch this
Code Red Worm

• Exploited IIS buffer overflow
• Floods network
• Attacks other servers
• Has dormant phase (so it might be there on your restore)
• http://www.cert.org/advisories/CA-2001-19.html
Code Red Cure

• This was ugly!
• Take server offline
• Try a restore (depending on damage)
• Run virus scan in all cases
Nimda

• Builds on Code Red Trojan
• Attacks web content files
• Can spread via HTML
• Can attack open shares
• Can overwrite executables (.exe)
• Can spread via email

Nimda Cure

- Like Code Red
- Take server offline
- Restore (maybe)
- Scan (for sure)
- Watch out for corrupted EXEs
  - Remember my ill formed apps…
Nimbda

- Maintenance was available months before the crisis
- Caught us with an “about to be replaced” IIS server
- Attacked Instructor File Server on same subnet
- Replaced executable files in “ill formed” applications
- Nasty to get rid of
  - Did restore
  - Scanned
  - Even deleted some directories
Myparty

- Attachment is an executable program
- Overwrites files
- Leaves backdoor auto start
- Sends itself to others
Hello!

My party... It was absolutely amazing!
I have attached my web page with new photos!
If you can please make color prints of my photos. Thanks!
Myparty Cure

- Devious
  - First pass attachment was an .exe
  - Second pass was a .com
    - Looked like a URL
- Virus scans catch
- Maintenance on Outlook detects
- May have subsided
  - Rumor that it only worked Jan. 27-29
General What To Do

• Don’t open that attachment!
• Apply maintenance
  – To Office
    • Especially Outlook
  – To Exchange
  – To IIS
  – To OS
• Run a virus scan program
  – Keep it current
General What To Do

• Secure your system
  – http://personal.cfw.com/~tkprit/inet/secure.html

• Good passwords

• Use ACLs to restrict access
What Next?

- Automate detection of attacks
  - SNORT intrusion detection
- Automate correction?
  - HOGWASH to neutralize attacks
- Where should firewalls play?
  - University “freedom” issue
  - Question of effectiveness
- University-wide license for Norton AntiVirus
Intrusion Detection

• It helps to know when something is happening
• Detection can identify known problems
• Suggests a solution
• First step to taking action
• May be useful in setting up a shill
Automated Response

• Can take action quickly
• Can prevent a crisis
• Need to recognize attack first
• Need to know of a corrective action that works
Two Approaches

• Inline packet capture
  – Two network cards
  – Read and forward each packet

• Parallel packet review
  – One network card
  – Watch packets as they go by
Inline

• Capture each packet and examine
• Can send out alert
• Can modify the packet
• Can take corrective action
  – Reset session
• This has performance implications
• Must allow promiscuous network connection
Parallel

- Watch packets as they go by
- Send out alert if you recognize a problem
- Can take action such as a session reset
- Must be quick
- Not the performance impact
- Must allow promiscuous network connection
Firewalls

• Contrary to University mindset
  – Open is good
  – Sharing is good
• Some argument about effectiveness
• Disagreement about need
• Much better than no defense
• Under consideration where appropriate
Microsoft and Security?

• Microsoft Strategic Technology Protection Program
  – Focus on security for Windows
  – Providing security toolkit for NT prior to XP

• Windows XP automated update capability
What Have We Learned?

• In spite of good effort, can get hit
• In spite of good effort, can look bad
• File servers need to be scanned, too
• Poorly designed applications are a liability
  – Self modifying code
  – Writing & Sharing information in executable directory
  – Makes share open for attack
• Attacks are more frequent and smarter
• They’ve discovered Windows
What Have We Learned?

• Locking down student machines isn’t good enough
• Even if it’s free, people still don’t use antivirus scan software
• No matter how often you tell them, they will open that attachment
• Windows is not necessarily more vulnerable
Open Issues

• Scan user files on servers?
  – Size issue
  – Performance issue
  – Privacy issue

• Deal with multiple mail products?

• Deal with “Ill Formed” applications?

• Firewall initiative?
  – Cost
  – Resistance to control of freedom
Resources

• Carnegie Mellon Software Engineering Institute
  – http://www.cert.org/nav/index_main.html

• Virus Encyclopedia
  – http://www.avp.ch/avpve/

• Computer Virus Help
  – http://pages.prodigy.net/henri_delger/

• IBM Antivirus Research
Resources

• DOE Computer Incident Advisory Capability
  – http://www.ciac.org/ciac/

• Microsoft
  – http://www.microsoft.com/security/
Questions?

It could be worse!
Corollary: It probably will be.