

## Malicious Code: Worms, Viruses and other Nasty “Bugs”



## What are the business risks?

- | Prevent computers from working resulting in lost billable hours.
- | Interrupt email communication sometimes for days at a time.
- | Threat to confidentiality if a virus randomly sends data files.
- | Damage credibility with clients.
- | Disable the network in the same way as a fire or other disaster would.

## What is malicious code?

- | Malicious code is a program that can spread across computers, networks and the internet by making copies of itself, usually without the user's knowledge.
- | There are many types of malicious code: Worms, Trojan horses and viruses.
- | For discussion, we will call them “Bugs”

## How do bugs infect computers?

- | Viruses may attach themselves to other programs or hide in code that is run automatically when you open certain types of files.
- | Certain types of code used by web pages can drop a virus onto your computer.
- | Worms can enter your computer directly from the internet without your assistance.
- | Viruses can run just by opening an email in Outlook, without clicking on any attachments.

## How Bugs Abuse Outlook

- | Hijack Outlook sending messages to everyone in your Contacts List.
- | Replace the “From” entry in email to random people from your contacts list.
- | Send an old email to everyone in your Contacts List with the virus attached.
- | The Preview Pane will automatically launch a virus without your help – don't use it.
- | And tomorrow...

## Symptoms of Infection

- | After clicking on an email attachment, dialog boxes appear or a sudden degradation in system performance occurs.
- | An antivirus program is disabled for no reason and it cannot be restarted.
- | Strange dialog boxes or message boxes appear onscreen.
- | New icons appear on the desktop that you did not put there, or are not associated with any recently installed programs.
- | Strange sounds or music play from the speakers unexpectedly.
- | A program disappears from the computer, but you did not intentionally uninstall it.
- | Computer will not start up normally
- | Programs, such as Word or Excel, become unstable
- | Response is degraded making computer seem sluggish

## What can these bugs do?

- | Display annoying messages
- | Launch pranks
- | Deny access to the computer or network
- | Corrupt, steal or delete data
- | Disable hardware
- | Hijack Outlook
- | Hijack your computer, turning it into a Spam Zombie
- | Record keystrokes
- | Disable email gateway
- | Disable firm network
- | Disable the internet

## Where do the risks lie?

- | Floppy disks and CD's
- | Documents and spreadsheets
- | Email – both in attachments and the body of the message
- | Programs
- | The internet – downloaded programs or files may be infected, web sites may push code down to your computer.
- | File sharing networks
- | Instant Messaging

## Risks at Home

- | Home PC's do not benefit from the vigilance of corporate virus protection including firewalls, virus protection software and regular system updates.
- | Kids visit web sites, share music files, download programs.
- | Home computers with "always on" broadband connections and no firewalls are obvious targets for hackers.
- | Wi-Fi – wireless signals extend beyond the home where they can be accessed by other computers.
- | KTC Documents pulled outside the secure office network can be picked up by crawlers and information distributed.

## Help for Home

- | If you work on your home computer or laptop, you have a responsibility to secure it.
- | Come to one of our home computer protection meetings .
- | Family members are welcomed and even encouraged to attend.
- | Visit the Training Corner of KTC Net

## More Bad News

- | Fraudulent emails
- | Pop ups
- | Spy ware
- | Instant messaging
- | Internet hot spots

## What do we do?

- | Keep current anti-virus software and firewalls running on the network at all times.
- | Keep PC's updated with latest security patches.
- | Block files with executable extensions.
- | Use Erado to grab suspicious email.
- | Subscribe to virus alert services.
- | Stay in contact with other firms nationwide to anticipate attacks.
- | Educate employees on the risks and prevention strategies.

## What can you do?

- | Don't trust attachments from anyone – even your biggest client, your spouse or your best friend.
- | If you weren't expecting it, don't open the attachment or the message.
- | If you get an attachment, call the sender or send a *new* email (don't open the one in question) confirming it was intended.
- | If you send attachments frequently, come up with a code to stick in the subject line so you can circumvent above.
- | Don't check your Yahoo, AOL or other third party email from the office, it is not scanned by Erado or our virus software.
- | Don't let clients or others use your computer to access the internet.
- | Don't download "helpful" tools from the web.
- | Don't attach your laptop to an unknown network without a firewall on it.
- | Protect your home computer.
- | Change your password often and make it a good one.
- | At home, consider using Netscape or other browser and don't use Outlook or Outlook Express.

## Is it really such a big deal?

- | The Slammer, Blaster, and Sobig families of worms, which paralyzed the Internet in 2003, are estimated to have caused \$12 to \$13 billion in damages.
- | In 2003, 64 percent of companies experienced one or more cyber security breaches (including KTC).
- | Given the pace of virus development, we are probably going to see even nastier criminal attacks in the future.
- | Future terrorist attacks may include computer viruses.
- | The Homeland Security Department has stated that cyber security is part of corporate fiduciary responsibility.

## In Conclusion

- | We owe it to our clients to do all we can to protect ourselves.



#514296