by Dave Murphy

Computer Viruses: an executive overview

Introduction

This white paper is for business owners and IT professionals.

It is an overview of the most common computer virus effects and simple, low-cost options for protecting valuable IT resources.

Most computer users, including many Information Technology (IT) professionals, don't fully understand the difference amongst computer viruses, Trojan horses, worms, and other types of computer-borne infections.

Introduction & history of viruses

Computer viruses can first be traced to the Pakistani Brain virus of the mid-nineteen eighties. The Brain virus was a boot sector virus (defined below), as legend has it, authored by the Amjad brothers, who were frustrated with computer piracy.

Since then, the term "computer virus" has become a common term wherever computers are used, especially personal computers. The media picks up and distorts reports of new viruses, such as the Melissa and BubbleBoy viruses of 1999. While each of these caused significant damage and loss of information, antivirus software was quickly updated to detect both viruses and counter their effects. However, the lasting effects caused by the media exposure only served to fuel the business culture's fascination with the potential danger of these viruses.

The most costly type of virus-caused data error is loss of accuracy.

While most people, including information managers fear that and therefore prepare for the worst case scenario of a virus' reformatting a hard disk or deleting masses of data files, these are actually not the effects on which we should place our greatest attention. It's a rather simple matter to maintain current data backups on tape or other media to restore data following a complete loss. In any regard, complete and current backups should be kept to repair honest, human data errors commonly caused by ill-trained or novice employees.

The most costly type of data loss is the *loss of accuracy*. Imagine a virus that infects only Microsoft Excel spreadsheets and exchanges every digit 2 and 3 it finds in each sheet. Numbers, formulae, and bottom-line figures would no longer be accurate, and the combined effect could easily lead to a magnitude offset.

Another embarrassing effect of some viruses is the release of confidential documents to Internet websites, newsgroups, and email lists. Or the attribution of your name to a false document that is published on the Internet. In either case, the public reaction to the virus' effect can ruin your reputation and your company's credibility.

What is a computer virus?

A computer virus is designed to replicate. It promulgates itself to other computer media (hard drives, floppy diskettes, tapes, ZIP disks, off-line and near-line storage systems) and then effects a transfer to another computer system and continues the self-replication process.

Until all instances of the virus are detected and destroyed, the virus maintains the capability of self-replication and the process can start all over again.

What's a payload?

Computer-borne infections usually contain a "payload," the action to be carried out. The virus is actually just the messenger, it's the payload that causes the actual damage.

Payloads can vary in their effect: from simple screen messages to data alterations, hard drive formatting, and even flash BIOS (Basic Input/Output System) reprogramming that effectively destroys the data, software, and hardware of a computer system.

How do I get a virus?

Viruses can be hidden in software programs and delivered by floppy disk, CD, email attachment, or directly via a network connection.

Once the virus infects a system, it begins the replication process of attaching itself to other files, disks, and systems.

There are three common families of computer viruses: macro, boot, and parasitic.

Macro viruses

Made common with the release of Microsoft Office's macro programing language, macro viruses infect data files such as word processing documents, spreadsheets, graphic presentations, and databases.

A macro is a set of instructions, like a simple computer program. These instructions can be executed very quickly with a single initiation command.

Macro viruses usually replicate themselves into other data files of the same type as well as startup configuration files so that they can quickly and easily transfer their payload to the system without being detected.

Any data file on an infected system uses the same host application will usually become infected. If the infected computer is on a network, connected to the Internet, or if the user shares these data files via other media, the virus can quickly spread.

Boot sector viruses

Most computers are self starting [they are able to pull themselves up by their own bootstraps]. The first section of a computer's hard disk is called the *boot sector*. It's within this storage area the computer looks for the commands necessary to continue the process of booting.

Viruses that attack this specific area of the disk are called boot sector viruses.

Boot sector viruses are especially effective at damaging information systems because they can prevent a computer system from starting properly. Many IT managers have become complacent and are lax in following the Cardinal rule of always having a virus-free, write-protected boot diskette available for each PC. With this diskette, a well-trained antivirus technician can boot the system, eradicate the virus, and repair the boot sector files.

Parasitic viruses

Parasitic viruses attach themselves to executable programs. When the program is executed either directly by the user or indirectly by another application, the virus can be launched.

On a computer network this can be especially damaging because computer files are often given specific access permissions, sometimes referred to as "rights."

IT managers are complacent and fail to follow the Cardinal rule.

Networks assign parasitic viruses the same access rights as the infected file. Therefore, a high-level infected file may release a parasitic virus with enough rights to damage hundreds of thousands of other files before being detected and destroyed.

Prevention

To prevent virus infection:

1) never use any external media (floppy diskette, CD, ZIP, etc.)

2) never connect to a computer network

3) never use a modem

4) never connect to the Internet

Realistically, none of these steps are possible.

Security against virus attack requires a reasonable level of attention to procedures, a good understanding of how viruses work, and a grasp of popular security practices.

A reasonable and sound antivirus policy should include:

1) daily backup of all data files and software applications. (If a virus does attack, corrupted files can be deleted and restored from the previous evening's backup media.)

2) Train all computer users of the effect of viral infection. Teach them how to detect viruses, and most of all, how to minimize the opportunity for viruses to invade their systems.

3) Create a written policy, preferably on a poster-sized wall hanging that describes good security practices and warns all to be vigilant to potential infections: floppy disks, downloaded Internet files, and email attachments being the most common transfer media.

4) Purchase and install a first-rate antivirus software and keep it updated each week.

Recommended antivirus software

ITrain recommends McAfee VirusScan. It's available worldwide in computer software retailers, and near-weekly updates are posted to the Network Associates' website: http://www.nai.com/.

Questions and comments

If you have any questions or if I may help you in any way, please call me at the ITrain offices. My direct email address is member@itrain.org.

Best regards in staying virus free,

ITrain
International Association of
Information Technology Trainers

PMB 451
6030-M Marshalee Dr
Elkridge, MD 21075-5935
1.888.290.6200 or 410.290.7000
603.925.1110 (fax)
itrain.org member@itrain.org