Computer Systems Technology

==

NIST Special Publication

Computer Viruses and Related Threats: A Management Guide

John P. Wack

Lisa J. Carnahan

Table of Contents

Executive Summary

Computer viruses and related threats represent an increasingly serious security problem in computing systems and networks. This document presents guidelines for preventing, deterring, containing, and recovering from attacks of viruses and related threats. This section acquaints senior management with the nature of the problem and outlines some of the steps that can be taken to reduce an organization's vulnerability.

What Are Computer Viruses and Related Threats?

Computer viruses are the most widely recognized example of a class of programs written to cause some form of intentional damage to computer systems or networks. A computer virus performs two basic functions: it copies itself to other programs, thereby *infecting* them, and it executes the instructions the author has included in it. Depending on the author's motives, a program infected with a virus may cause damage immediately upon its execution, or it may wait until a certain event has occurred, such as a particular date and time. The damage can vary widely, and can be so extensive as to require the complete rebuilding of all system software and data. Because viruses can spread rapidly to other programs and systems, the damage can multiply geometrically.

Related threats include other forms of destructive programs such as Trojan horses and network worms. Collectively, they are sometimes referred to as *malicious software*. These programs are often written to masquerade as useful programs, so that users are induced into copying them and sharing them with friends and work colleagues. The malicious software phenomena is fundamentally a people problem, as it is authored and initially spread by individuals who use systems in an unauthorized manner. Thus, the threat of unauthorized use, by unauthorized *and* authorized users, must be addressed as a part of virus prevention.

What Are the Vulnerabilities They Exploit?

Unauthorized users and malicious software may gain access to systems through inadequate system security mechanisms, through security holes in applications or systems, and through weaknesses in computer management, such as the failure to properly use existing security mechanisms. Malicious software can be copied intentionally onto systems, or be spread when users unwittingly copy and share infected software obtained from public software repositories, such as software bulletin boards and shareware. Because malicious software often hides its destructive nature by performing or claiming to perform some useful function, users generally don't suspect that they are copying and spreading the problem.

Why Are Incidents of Viruses and Related Threats On the Rise?

Viruses and related threats, while not a recent phenomena, have had relatively little attention focused on them in the past. They occurred less frequently and caused relatively little damage. For these reasons, they were frequently treated lightly in computer design and by management, even though their potential for harm was known to be great.

Computer users have become increasingly proficient and sophisticated. Software applications are increasingly complex, making their bugs and security loopholes more difficult to initially detect and correct by the manufacturer. In conjunction with these two factors, some brands of software are now widely used, thus their bugs and security loopholes are often known to users. With the widespread use of personal computers that lack effective security mechanisms, it is relatively easy for knowledgeable users to author malicious software and then dupe unsuspecting users into copying it.

Steps Toward Reducing Risk

Organizations can take steps to reduce their risk to viruses and related threats. Some of the more important steps are outlined below.

- Include the damage potential of viruses, unauthorized use, and related threats in risk analysis and contingency planning. Develop a plan to deal with potential incidents.

- Make computer security education a prerequisite to any computer use. Teach users how to protect their systems and detect evidence of tampering or unusual activity.

- Ensure that technically oriented security and management staff are in place to deal with security incidents.

- Use the security mechanisms that exist in your current software. Ensure that they are used correctly. Add to them as necessary.

- Purchase and use software tools to aid in auditing computing activity and detecting the presence of tampering and damage.

1. Introduction

This document provides guidance for technical managers for the reduction of risk to their computer systems and networks from attack by computer viruses, unauthorized users, and related threats. The guidance discusses the combined use of policies, procedures, and controls to address security vulnerabilities that can leave systems open to attack. The aim of this document is not to provide solutions to the wide range of specific problems or vulnerabilities, rather it is to help technical managers administer their systems and networks such that manifestations of viruses and related threats can be initially prevented, detected, and contained.

1.1 Audience and Scope

This document is intended primarily for the managers of multi-user systems, personal computers, and associated networks, and managers of end-user groups. Additionally, the document is useful for the users of such systems. The document presents an overview of computer viruses and related threats, how they typically work, the methods by which they can attack, and the harm they can potentially cause. It then presents guidance in the following areas:

- *Multi-User Systems and Associated Networks* - with guidance directed at managers of medium to small systems (as opposed to mainframes that already provide generally effective security controls or are by their nature more secure) and associated wide area and large local area networks, as well as managers of end-users of such systems
- *Personal Computer Systems and Networks* - guidance is directed at those responsible for the management of personal computers and personal computer networks, as well as the managers of personal computer end-users

Within these general categories, individual computing environments will vary widely, from size of computer to user population to type of software and computing requirements. To accommodate these differences, the guidance presented here is general in nature. It attempts to address computer security problems and vulnerabilities that are likely to be found in most computing environments. This document does not address problems directly related to specific brands of software or hardware. A reading list at the end of the document contains references and pointers to other literature that address specific systems and software.

Recommended control measures are grouped according to categories that include general policies and procedures, education, software management, technical controls, monitoring, and contingency planning. The guidance emphasizes the need for a strong security program as a means for protection from manifestations of viruses and related threats, and as a means for providing detection, containment, and recovery. Such a security program requires personal involvement on the part of management to ensure that the proper policies, procedures, and technical controls exist, and that users are educated so that they can follow safe computing practices and understand the proper actions to take if they detect the presence of viruses or related threats. The guidelines recommend that network managers, multi-user system managers, end-users, and end-user managers work with each other and approach virus protection from an organizationally consistent basis.

1.2 How to Use This Guide

This document is divided into five chapters and two appendices. Chapter 2 describes in general how viruses and related software operate, the vulnerabilities they exploit, and how they can be introduced into systems and networks. Chapter 3 discusses general protection strategies and control measures that apply to technical and end-user management in general; this is done so that the same guidance need not be repeated for each of the succeeding chapters that deal with specific environments. Chapters 4 and 5 present guidance specific to multi-user and personal computer environments, respectively. The guidance in these chapters is directed at the respective technical managers and managers of associated networks, as well as the managers of end-user groups that use such systems and networks. It is recommended that all readers, regardless of their management perspective, examine Chapters 3, 4, and 5 to gain a fuller appreciation of the whole environment with regard to threats, vulnerabilities, and controls.

Appendix A contains document references, while Appendix B contains a reading list with references to general and specific information on various types of viruses, systems, and protective measures. Readers can use these documents to obtain information specific to their individual systems and software.

2. A Brief Overview on Viruses and Related Threats

The term *computer virus* is often used in a general sense to indicate any software that can cause harm to systems or networks. However, computer viruses are just one example of many different but related forms of software that can act with great speed and power to cause extensive damage - other important examples are Trojan horses and network worms. In this document, the term *malicious software* refers to such software.

2.1 Trojan Horses

A Trojan horse[1] program is a useful or apparently useful program or command procedure containing hidden code that, when invoked, performs some unwanted function. An author of a Trojan horse program might first create or gain access to the source code of a useful program that is attractive to other users, and then add code so that the program performs some harmful function in addition to its useful function. A simple example of a Trojan horse program might be a calculator program that performs functions similar to that of a pocket calculator. When a user invokes the program, it appears to be performing calculations and nothing more, however it may also be quietly deleting the user's files, or performing any