December 2005

INFORMATION TECHNOLOGY LABORATORY

Bulletin

ADVISING USERS ON INFORMATION TECHNOLOGY

PREVENTING AND HANDLING MALWARE INCIDENTS: HOW TO PROTECT INFORMATION TECHNOLOGY SYSTEMS FROM MALICIOUS CODE AND SOFTWARE

Shirley Radack, Editor
Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology

The term *malware* is used to describe malicious code and malicious software that are covertly inserted into an information technology (IT) system to compromise the confidentiality, integrity, or availability of the data, applications, or operating system, or to annoy or disrupt the system's owner. Malware incidents are a significant external threat to the security of many IT systems, often causing widespread damage and disruption, and forcing users and organizations to carry out extensive, costly efforts to restore system security.

Malware includes five categories of inserted programs: viruses, worms, Trojan horses, malicious mobile code, and blended attacks. Viruses and worms are usually designed to carry out their functions without the user's knowledge. Blended attacks use a combination of techniques to insert malicious programs. Malware also includes other attacker tools such as backdoors, rootkits, and keystroke loggers, and tracking cookies which are used as spyware. Spyware, when inserted into a user's system, threatens personal privacy and enables the attacker to monitor personal activities and to carry out financial fraud.

Guide to Malware Incident Handling and Prevention: Recommendations of the National Institute of Standards and Technology

NIST's Information Technology Laboratory recently published NIST Special Publication (SP) 800-83, *Guide to Malware Incident Handling and Prevention: Recommendations of the National Institute of Standards and Technology*. The guide assists organizations and users in planning and implementing security programs to prevent potential malware incidents and to limit damage from unforeseen incidents that might occur.

Written by Peter Mell of NIST and Karen Kent and Joseph Nusbaum of Booz Allen Hamilton, NIST SP 800-83 discusses the different types of malware and recommends prevention and incident handling techniques. The appendices provide additional resources on malware prevention and handling methods, and include detailed techniques and scenarios. A glossary of the many specialized terms used in the guide, a list of acronyms, and an extensive reference list of print and online resources are also provided. The publication is available in electronic format from NIST's website: http://csrc.nist.gov/publications/nistpubs/index.html.

Malware: What it is

Malware includes the following major categories of malicious code and programs:

- **Viruses** are self-replicating codes that insert copies of the virus into host programs or data files. Viruses often result from user interactions, such as opening a file or running a program, and include:

(Continued on Page 2)

ITL Bulletins are published by the Information Technology Laboratory (ITL) of the National Institute of Standards and Technology (NIST). Each bulletin presents an in-depth discussion of a single topic of significant interest to the information systems community. Bulletins are issued on an as-needed basis and are available from ITL Publications, National Institute of Standards and Technology, 100 Bureau Drive, Stop 8900, Gaithersburg, MD 20899-8900, telephone (301) 975-2832. To be placed on a mailing list to receive future bulletins, send your name, organization, and business address to this office. You will be placed on this mailing list only.

Bulletins issued since August 2004:

- *Electronic Authentication: Guidance for Selecting Secure Techniques*, August 2004
- *Information Security Within the System Development Life Cycle*, September 2004
- *Securing Voice Over Internet Protocol (IP) Networks*, October 2004
- *Understanding the New NIST Standards and Guidelines Required by FISMA*, November 2004
- *Integrating IT Security into the Capital Planning and Investment Control Process, January 2005*
- *Personal Identity Verification (PIV) of Federal Employees and Contractors: Federal Information Processing Standard (FIPS) 201 Approved by the Secretary of Commerce*, March 2005
- *Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule,* April 2005
- *Recommended Security Controls for Federal Information systems: Guidance of Selecting Cost-effective Controls Using a Risk-based Process, May 2005*
- *NIST's Security Configuration Checklists Program for IT Products,* June 2005
- *Implementation of FIPS 201, Personal Identify Verification (PIV) of Federal Employees and Contractors, August 2005*
- *Biometric Technologies: Helping to Protect Information and Automated Transactions I Information Technology Systems, September 2005*
- *National Vulnerability Database: Helping Information Technology System Users and Developers Find Current Information About Cyber Security Vulnerabilities,* October 2005
- *Securing Microsoft Windows XP Systems: NIST Recommendations for Using a Security Configuration Chccklist,* November 2005

- **Compiled viruses** that are executed by an operating system. These include file infector viruses, which attach themselves to executable programs; boot sector viruses, which infect the master boot records of hard drives or the boot sectors of removable media; and multipartite viruses, which combine the characteristics of file infector and boot sector viruses.
- **Interpreted viruses** that are executed by an application. These include macro viruses that take advantage of the capabilities of the macro programming language to infect application documents and document templates; and scripting viruses that infect scripts and are understood by scripting languages processed by services on the operating system.

- **Worms** are self-replicating, self-contained programs that usually perform without user intervention. Worms create fully functional copies of themselves, and they do not require a host program to infect a system. Attackers often insert worms because they can potentially infect many more systems in a short period of time than a virus can. Worms include:
  - **Network service worms** that take advantage of vulnerabilities in network services to propagate and infect other systems.
  - **Mass mailing worms** that are similar to e-mail–borne viruses but are self-contained, rather than infecting an existing file.

- **Trojan horses** are self-contained, non-replicating programs that appear to be benign, but that actually have a hidden malicious purpose. Trojan horses either replace existing files with malicious versions or add new malicious files to systems. They often deliver other attacker tools to systems.

- **Malicious mobile code** is software with malicious intent that is transmitted from a remote system to a local system. The inserted programs are executed on the local system, usually without the user's explicit instruction. Programs delivered in this way can be used by many different operating systems and applications, such as web browsers and e-mail clients. Although the mobile code may be benign, attackers use it to transmit viruses, worms, and Trojan horses to the user's workstation. Malicious mobile code does not infect files or attempt to propagate itself, but exploits vulnerabilities by taking advantage of the default privileges granted to mobile code. Languages used for malicious mobile code include Java, ActiveX, JavaScript, and VBScript.

- **Blended attacks** use multiple methods of infection or transmission. A blended attack could combine the propagation methods of viruses and worms.

- **Tracking cookies** are persistent cookies that are accessed by many websites, allowing a third party to create a profile of a user's behavior. Tracking cookies are often used in conjunction with web bugs, which are tiny graphics on websites and which are referenced within the HTML content of a web page or e-mail. The purpose of the graphic is to collect information about the user viewing the content.

Who We Are

The Information Technology Laboratory (ITL) is a major research component of the National Institute of Standards and Technology (NIST) of the Technology Administration, U.S. Department of Commerce. We develop tests and measurement methods, reference data, proof-of-concept implementations, and technical analyses that help to advance the development and use of new information technology. We seek to overcome barriers to the efficient use of information technology, and to make systems more interoperable, easily usable, scalable, and secure than they are today. Our website is http://www.itl.nist.gov.

- **Attacker tools** might be delivered to a system as part of a malware infection or other system compromises. These tools allow attackers to have unauthorized access to or use of infected systems and their data, or to launch additional attacks. Popular types of attacker tools include:
  - **Backdoors** are malicious programs that listen for commands on a certain TCP or UDP port. Most backdoors allow an attacker to perform a certain set of actions on a system, such as acquiring passwords or executing arbitrary commands. Backdoors include zombies (also known as bots), which are installed on a system to cause it to

ITL Bulletins Via E-Mail

We now offer the option of delivering your ITL Bulletins in ASCII format directly to your e-mail address. To subscribe to this service, send an e-mail message from your business e-mail account to listproc@nist.gov with the message **subscribe itl-bulletin**, and your name, e.g., John Doe. For instructions on using listproc, send a message to listproc@nist.gov with the message HELP. To have the bulletin sent to an e-mail address other than the FROM address, contact the ITL editor at 301-975-2832 or elizabeth.lennon@nist.gov

attack other systems, and remote administration tools, which are installed on a system to enable a remote attacker to gain access to the system's functions and data.

- **Keystroke loggers** monitor and record keyboard use. Some require the attacker to retrieve the data from the system, while other loggers actively transfer the data to another system through e-mail, file transfer, or other means.
- **Rootkits** are collections of files that are installed on a system to alter its standard functionality in a malicious and stealthy way. A rootkit can make many changes to a system to hide the rootkit's existence, making it very difficult for the user to determine that the rootkit is present and to identify what changes have been made.
- **Web browser plug-ins** provide a way for certain types of content to be displayed or executed through a web browser. Attackers often create malicious web browser plug-ins that act as spyware and monitor the use of the browser.
- **E-mail generators** are programs that can be used to create and send large quantities of e-mail, such as malware, spyware, and spam, to other systems without the user's permission or knowledge.
- **Attacker toolkits** include several different types of utilities and scripts that can be used to probe and attack systems, such as packet sniffers, port scanners, vulnerability scanners, password crackers, remote login programs, and attack programs and scripts.

- **Common non-malware threats associated with malware** include phishing, which uses computer-based means to trick users into revealing financial information and other sensitive data. Phishing attacks frequently place malware or attacker tools on systems. Virus hoaxes, which are false warning of new malware attacks, are another common threat.

Recommendations for Preventing Malware Incidents

Organizations should protect their information and information systems from malware through their ongoing IT security planning, management, and implementation activities. NIST recommends that organizations take the following actions to prevent malware incidents and to respond effectively and efficiently to any attacks that might occur.

Develop and implement an approach to malware incident prevention, based on the attack methods that are most likely to be used, both currently and in the near future. Choose prevention techniques that are appropriate to the computing environment and system, and provide for policy statements, awareness programs for users and IT staff, and vulnerability and threat mitigation efforts.

Ensure that policies support the prevention of malware incidents and provide for user and IT staff awareness, vulnerability mitigation, and security tool deployment and configuration. Malware prevention should be stated clearly in policies, which should be as general as possible to allow for flexibility in implementation and to reduce the need for frequent updates. At the same time, policy statements should be specific enough to make their intent and scope clear and to achieve consistent and effective results. Policies should include provisions that are applicable to remote workers, both those using systems controlled by the organization and those using systems outside of the organization's control such as contractor computers, home computers, computers of business partners, and mobile devices.

Incorporate malware incident prevention and handling into awareness programs and provide guidance and training to users. Users should be alerted to the ways that malware spreads, the risks that malware poses, the inability of technical controls to prevent all incidents, and the role of users in preventing incidents. Users should be aware of policies and procedures for incident handling, including how to detect malware on a computer, how to report suspected infections, and what can be done to assist the incident handlers.

Establish capabilities to mitigate vulnerabilities and to help prevent malware incidents through documented policy, technical processes, and procedures. Appropriate techniques or combinations of techniques should be used for patch management, application of security configuration guides and checklists, and host protection to address vulnerabilities effectively.

Establish threat mitigation capabilities to assist in containing malware incidents by detecting and stopping malware before it can affect systems. NIST strongly recommends that organizations install antivirus software on all systems when such software is available. Other technical controls that can be used are intrusion prevention systems, firewalls, routers, and certain application configuration settings.

Establish a robust incident response process capability that addresses malware incident handling through preparation, detection and analysis, containment/eradication/recovery, and post-incident activities.

- **Preparation.** Develop malware-specific incident handling policies and procedures. Regularly conduct malware-oriented training and exercises;

designate a few individuals or a small team to be responsible for coordinating the organization's responses to malware incidents. Establish several communication mechanisms so that coordination among incident handlers, technical staff, management, and users can be sustained if an attack occurs.

- **Detection and Analysis.** Monitor malware advisories and alerts produced by technical controls, such as antivirus software, spyware detection and removal utilities, and intrusion detection systems, to identify impending malware incidents. Review malware incident data from primary sources such as user reports, IT staff reports, and technical controls to identify malware-related activity. Construct trusted toolkits on removable media that contain up-to-date tools for identifying malware, listing currently running processes and performing other analysis actions. Establish a set of prioritization criteria that identify the appropriate level of response for various malware-related incidents.

- **Containment.** Decide who has the authority to make major containment decisions, when actions are appropriate, and the methods of containment that will be employed. Early containment can help stop the spread of malware and prevent further damage to systems. Strategies and procedures for making containment-related decisions should reflect the level of risk acceptable to the organization.

  Provide users with instructions on how to identify infections and what measures to take if a system is infected, but do not rely primarily on users for containing malware incidents. Use updated antivirus software and other security tools to contain incidents. Submit copies of unknown malware to security software vendors for analysis and contact trusted parties, such as incident response organizations and antivirus vendors, when guidance is needed on handling new threats.

  Be prepared to shut down or block services such as e-mail or Internet access to contain a malware incident and understand the consequences of doing so. Be prepared to respond to problems caused by other organizations disabling their own services in response to a malware incident. Identify those hosts infected by malware, considering users who have remote access to systems and mobile users.

- **Eradication.** Be prepared to use combinations of eradication techniques simultaneously for different situations to remove malware from infected systems. Support awareness activities to inform users about eradication and recovery efforts.

- **Recovery.** Restore the functionality and data of infected systems and lift temporary containment measures. Consider possible worst-case scenarios and determine how recovery should be performed, including rebuilding compromised systems from scratch or known good backups. Determine when to remove temporary containment measures, such as suspension of services or connectivity. Containment measures should be kept in place until the number of infected systems and systems vulnerable to infection is sufficiently low that subsequent incidents should be of little consequence. The incident response team should assess the risks of restoring services or connectivity and report to organization managers, who are responsible for assessing the business impact of maintaining the containment measures and for determining actions to be taken concerning containment.

- **Post-Incident Activity.** Conduct an assessment of lessons learned after major malware incidents to prevent similar future incidents. Identify needed changes to security policy, software configurations, and the implementation of malware detection and prevention controls.

Establish malware incident prevention and handling capabilities that address current and short-term future threats and that are robust and flexible. Maintain awareness on the latest threats and the security controls that are available to combat each threat. Plan and implement appropriate controls, emphasizing the prevention of malicious incidents.

The use of malware, spyware, phishing attacks, and other attempts to collect personal information are expected to lead to future identity theft and financial fraud. Demands for better protection should drive the development of more robust spyware detection and removal utilities, and more effective antivirus software. But there is always a concern that better technical controls could make attackers even more resourceful and innovative in avoiding automated detection and taking advantage of the trust of users. Other future threats are viruses and worms that could attack PDA devices and cell phones, or that could use these devices as malware carriers. Organizations must always be aware of the latest threats and should be prepared to implement appropriate security controls to protect their IT systems.

More Information

The following Special Publications (SPs) provide help to organizations in planning and implementing effective security controls. These publications are available in electronic format from the NIST Computer Security Resource Center at http://csrc.nist.gov/publications.

NIST SP 800-28, *Guidelines on Active Content and Mobile Code*, discusses the security risks and security controls associated with the technology of active content.

NIST SP 800-31, *Intrusion Detection Systems (IDS)*, provides information on installing and using intrusion detection systems.

NIST SP 800-40, Version 2, *Creating a Patch and Vulnerability Management Program,* helps organizations establish patch and vulnerability management programs to protect IT systems from the exploitation of vulnerabilities.

NIST SP 800-42, *Guideline on Network Security Testing*, describes available security testing techniques, their strengths and weaknesses, and the recommended frequencies for testing as well as strategies for deploying network security testing.

NIST SP 800-45, *Guidelines on Electronic Mail Security*, describes secure practices for the installation, configuration, and maintenance of mail servers and clients.

NIST SP 800-53, *Recommended Security Controls for Federal Information Systems,* helps organizations to identify, select, and implement needed controls, including malware protection mechanisms for workstations, servers, mobile computing devices, firewalls, e-mail servers, and remote access servers.

NIST SP 800-61, *Computer Security Incident Handling Guide*, describes the four phases of the incident response process -- preparation, detection and analysis, containment/eradication/recovery, and post-incident activity.

Disclaimer: Any mention of commercial products or reference to commercial organizations is for information only; it does not imply recommendation or endorsement by NIST nor does it imply that the products mentioned are necessarily the best available for the purpose.

U.S. DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
100 Bureau Drive, Stop 8900
Gaithersburg, MD 20899-8900