ITL BULLETIN FOR SEPTEMBER 2013

ITL PUBLISHES GUIDANCE ON PREVENTING AND HANDLING MALWARE INCIDENTS

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) recently published guidance on preventing and handling malware incidents. Written by Murugiah Souppaya of NIST and Karen Scarfone of Scarfone Cybersecurity, NIST Special Publication 800-83 Revision 1, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops*, provides recommendations for improving an organization's malware incident prevention procedures. It also gives guidance on strengthening an existing incident response capability so that organizations are better positioned to handle malware incidents when they occur.

Also known as malicious code, *malware* refers to a program that is covertly inserted into another program with the intent to destroy data, run destructive or intrusive programs, or otherwise compromise the confidentiality, integrity, or availability of the victim's data, applications, or operating system. As the most common external threat to most hosts, malware can cause widespread damage and disruption of organizational information systems and requires extensive recovery efforts by the enterprise. Unlike malware threats of several years ago, many of today's malware threats are stealthy and quiet, slowly spreading throughout the network, gathering information over extended periods and resulting in loss of sensitive data and other compromises of data confidentiality.

In Special Publication 800-83 Revision 1, NIST recommends that federal agencies and private sector enterprises implement the following actions to strengthen their malware incident response:

- **Develop and implement an approach to malware incident prevention**. The approach should be based on current and future attack vectors and should be well suited to the organizational environment.

- **Ensure that organizational policies address malware incident prevention**. An organization's policy statements should be used as the basis for additional malware prevention efforts, such as staff awareness, vulnerability and threat mitigation, and defensive architecture. Policies should be general and flexible, yet specific and clear, and should consider remote users.

- **Incorporate the prevention and handling of malware incidents into awareness programs**. Make all users aware of how malware infects computers, the risks of malware, and the role of users in preventing incidents. Make users aware of policies and procedures and train IT staff.

- **Ensure vulnerability mitigation capabilities to help prevent malware incidents**. Document organizational policies and procedures to mitigate known vulnerabilities that could be exploited by malware. Use appropriate combinations of techniques for the most effective results.

- **Use threat mitigation capabilities to contain malware incidents**. Perform threat mitigation to detect and stop malware before it can reach its targets. Deploy antivirus software on all hosts. Use other technical controls such as intrusion prevention systems, firewalls, content filtering and inspection, and application whitelisting.

- **Use defensive architecture methods to lessen the impact of malware incidents**. Consider altering the defensive architecture of computer software to mitigate incidents. Use sandboxing, browser separation, and segregation through virtualization techniques.

- **Develop a resilient incident response capability that includes malware incident handling**. The incident response process has four steps: preparation, detection and analysis, containment or eradication and recovery, and post-incident activity. Preparation includes building malware-related skills, improving communications, and acquiring the necessary tools and resources. Detection and analysis involves analyzing incidents and validating that malware is the cause, identifying which hosts are involved, and prioritizing incident handling. Containment includes stopping the spread of malware and preventing further damage; eradication removes malware from infected hosts; and recovery involves restoring functionality and removing containment measures. Finally, post-incident activity consists of conducting a comprehensive assessment of lessons learned.

While malware incidents cannot be totally prevented, these recommendations can help organizations to prevent some attacks and to mitigate the damage when attacks occur. With today's interconnected information systems, strengthening organizational incident response capability to include malware incidents can go a long way to ensure the confidentiality, integrity, and availability of organizational information assets.

ITL Bulletin Publisher:
Elizabeth Lennon, Writer/Editor
Information Technology Laboratory
National Institute of Standards and Technology
Email elizabeth.lennon@nist.gov

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.