TMA Privacy and
Civil Liberties Office
Information Paper

MALICIOUS CODE OVERVIEW

Malicious Code ◆ February 2010

What is Malicious Code?

Malicious code is software that is purposely designed to do damage or cause unwanted behaviors in computer systems. It can corrupt files, erase hard drives, or enable a hacker to gain unauthorized access to computer systems. Malicious code is generally spread through e-mail attachments, downloading contaminated files from the Internet, or visiting an infected website which automatically downloads the malware. Some common indicators a device may have fallen victim to this type of software include automatic system reboots, missing files, unusual dialog boxes or error messages, programs that start slowly or do not run at all, and unanticipated noticeable changes to the systems after opening an e-mail attachment.

Responding to Malicious Code:

Any sign of a malicious code on a computer system should be reported to the local Information Assurance Officer (IAO) or Help Desk immediately. Additionally, the following steps should be taken to prevent the virus from spreading to the rest of the network:

- Disconnect the computer from the network, but do not turn it off.
- Contact the IAO or Help Desk and provide an incident description to include the date and time of the incident, any actions taken during the incident, the location of the incident including, if known, the IP address, machine name, and type of device involved.
- Place a notification on the device that clearly indicates the computer has been infected.

Types of Malicious Code:

There are numerous types of software that hackers employ in an attempt to gain access to computer systems, including:

- **Virus** – a program that replaces or alters one of the programs on a computer.
    - **Polymorphic virus** – a type of virus that changes itself slightly each time it affects a new computer, thus making it harder for anti-virus programs to detect and remove.
    - **Macro virus** – a type of virus that infects macro-based applications, such as word processors, by modifying the initialization sequence of the program.

  - **Trojan horse** – a type of virus that is hidden within an apparently harmless application, usually an executable file. The virus is installed as soon as the host application, such as a game, is executed.

- **Worm** – a specific type of code that actively attempts to spread itself to other computers, often by sending itself to every address in an e-mail address book.
- **Logic bomb** – a type of malware that executes and attacks the infected computer when a particular set of conditions is met, such as on a specific date or time.

Steps to Avoid Becoming a Victim:

The following are best practices that should be used to prevent becoming a victim of malicious code:

- Use caution when opening e-mail attachments, even when the e-mail came from a colleague.
- Forward suspicious e-mail messages to spam@tma.osd.mil without opening any attachments.
- Exercise concern when browsing the Internet, especially on unfamiliar websites.

Sources of Information:

- Defense Information Systems Agency, “DoD Information Assurance Awareness” October 2009, (http://iase.disa.mil/eta/iaav8/iaav8/index.htm).
- Military Health System Information Assurance Implementation Guide No. 3 “Incident Reporting and Response Program” 19 July 2005, (http://www.tricare.mil/tmis_new/ia/3%20-%20Incident%20Reporting%2020090608.pdf).
- United States Southern Command, “Beware of Hackers Network News”, 14 July 2006, (http://www.jtfgtmo.southcom.mil/wire/wire/WirePDF/v7/Issue17v7.pdf).