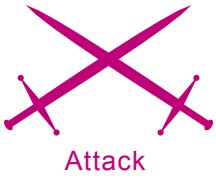

Analyzing Malicious Code

Hardik Shah
Anthony L. Williams

Difficulty

Computer networks and the Internet have been plagued by malicious code and its malevolent effects for long. This article will give you an introduction into the basic and practical usage of analyzing malware in a controlled environment.

Malicious code can be defined as *code that has been developed to perform various harmful activities on a normal computer.* Examples of such harmful activity can be actions such as stealing the end users data or personal information, infecting other machines on a network or sending spam through infected machines.

There are several categories of malicious code which include but are not limited to viruses, worms, trojan horses and bots. Each of these categories has differing characteristics according to their intended purpose. As we move forward, our aim is to discuss the various techniques we can use for effectively analyzing such malicious code.

Types of Malicious Code

Let us discuss the basic definitions of some different types of malicious code:

- *Virus*: Viruses are simple programs, which are written to change the way the computer works without the permission of its user. A virus cannot infect other PCs on a network until someone executes an infected file.
- *Trojan Horse*: In the context of computer software, a Trojan horse is a program that unlike a virus, contains or installs a malicious program (sometimes called the payload or 'Trojan') while under the guise of being something else.
- *Worms*: A computer worm is a self-replicating computer program. It uses the network to send copies of itself to other nodes (computer terminals on the network) and it may do it without any user intervention.

What you will learn...

- What malicious code is
- Tools and techniques used for malicious code analysis
- How to analyze the NetSky-P worm

What you should know...

- Elementary binary debugging techniques
- Packet analysis basics
- The Windows environment