REVIEW LESSON

MTA Course: 98-367 Security Fundamentals
Lesson name: Understand Operating System Security 2.6
Topic: Understand malware
(One 50-minute class period)
File name: SecurityFund_RL_2.6

Lesson Objective

2.6: Understand malware. *This objective may include, but is not limited to:* buffer overflows, worms, Trojans, spyware.

Preparation Details

Instructor preparation activities

- Register to view ***TechNet Webcast: Rootkits in Windows*** on-demand webcast and download a .wmv of the webcast now. By registering, you will also receive a confirmation email the following day with a link to the PPT download.
- Create a Windows Live® ID.
- Download a copy of "The Antivirus" Defense-in-Depth Guide (see links below).
- Download "What is Microsoft® Application Threat Modeling" (Hi-Res Video) (see links below).
- Download "Windows® Malicious Software Removal Tool" (see links below).

Resources, software, and additional files needed for this lesson

- SecurityFund_PPT_2.6
- SecurityFund_SA_2.6
- SecurityFund_SA_2.6_Key

Teaching Guide

Essential Vocabulary

bot—short for robot. A displayed representation of a person or other entity whose actions are based on programming. A program that performs some task on a network, especially a task that is repetitive or time consuming.

buffer overflow—one of the most notorious forms of attack from the Internet. They rely on the simple fact that programmers may make errors when reserving space for variables.

rootkit—collection of software programs that a hacker can use to gain unauthorized remote access to a computer and launch additional attacks. These programs may use a number of different techniques, including monitoring keystrokes, changing system log files or existing system applications, creating a backdoor into the system, and starting attacks against other computers on the network. Rootkits are generally organized into a set of tools that are tuned to specifically target a particular operating system.

spam—unsolicited e-mail generated to advertise some service or product. This phenomenon is generally considered a nuisance, but spam is not malware. However, the dramatic growth in the number of spam messages being sent is a problem for the infrastructure of the Internet that results in lost productivity for employees who are forced to wade through and delete such messages every day.

spyware—software sometimes referred to as spybot or tracking software. Spyware uses other forms of deceptive software and programs that conduct certain activities on a computer without obtaining appropriate consent from the user. These activities can include collecting personal information, and changing Internet browser configuration settings. Beyond being an annoyance, spyware results in a variety of issues that range from degrading the overall performance of your computer to violating personal privacy.

trojan—a program that appears to be useful or harmless but that contains hidden code designed to exploit or damage the system on which it is run. Trojan horse programs are most commonly delivered to users through e-mail messages that misrepresent the program's purpose and function. Also called Trojan code. A Trojan horse does this by delivering a malicious payload or task when it is run.

virus—uses code written with the express intention of replicating itself. A virus attempts to spread from computer to computer by attaching itself to a host program. It may damage hardware, software, or data. When the host is executed, the virus code also runs, infecting new hosts and sometimes delivering an additional payload.

worm—uses self-propagating malicious code that can automatically distribute itself from one computer to another through network connections. A worm can take harmful action, such as consuming network or local system resources, possibly causing a denial of service attack. Some worms can execute and spread without user intervention, while others require users to execute the worm code directly in order to spread. Worms may also deliver a payload in addition to replicating.

Lesson Sequence

Activating prior knowledge/lesson staging (Anticipatory Set: 10 minutes)

1. Use the downloaded video to introduce the Windows Application Threat Modeling concept. (Microsoft Download Center: What is Microsoft Application Threat Modeling *http://www.microsoft.com/downloads/details.aspx?FamilyID=29a6d444-9954-41f3-9666-3688417b5e08&displaylang=en)*
2. Show the video and ask students to record questions about concepts they do not fully understand.
3. As time permits, call on students to ask their questions.

Lesson activity (40 minutes)

1. Teacher Instruction (20 minutes)
   - Use the included PowerPoint® presentation to review concepts related to malware.
   - On slide8 a list of buffer overflow attacks is shown.
     - In pairs, students research an attack and report their findings.
     - Then give the students 2 minutes to discuss answers with a partner.
     - Finally, have each pair of students share their answers with the whole group.
     - Repeat for each additional entry.
2. Guided Practice (20 minutes; please see the "Web links" section regarding this assignment, slide 8)
   - Download the Microsoft Threat and Modeling tool from: *http://www.microsoft.com/downloads/details.aspx?familyid=59888078-9daf-4e96-b7d1-944703479451&displaylang=en*
   - Install the software tool and guide students through each step.

Assessment/lesson reflection (10 minutes)

1. Download the "Windows Malicious Software Removal Tool" *(http://www.microsoft.com/downloads/details.aspx?FamilyID=ad724ae0-e72d-4f54-9ab3-75b8eb148356&displaylang=en)*
2. Install and run the "Windows Malicious Software Removal Tool".
3. Share the results with the class.

Microsoft resources and Web links

- **Microsoft Download Center: The Antivirus Defense-in-Depth Guide**
  http://www.microsoft.com/downloads/details.aspx?FamilyId=F24A8CE3-63A4-45A1-97B6-3FEF52F63ABB&displaylang=en
- **Microsoft Download Center: What is Microsoft Application Threat Modeling (Hi-Res Video)**
  http://www.microsoft.com/downloads/details.aspx?FamilyID=29a6d444-9954-41f3-9666-3688417b5e08&displaylang=en
- **Protecting against buffer overflows**
  http://support.microsoft.com/kb/889741
- **Microsoft Download Center: Windows Malicious Software Removal Tool**
  http://www.microsoft.com/downloads/details.aspx?FamilyID=ad724ae0-e72d-4f54-9ab3-75b8eb148356&displaylang=en