Preparation for Handling Malware Incidents

Objectives:

At the end of this episode, I will be able to:

Understand what malware is, as well as the different types of malware that an IH&R team member may encounter.

Explain what the basic components of Malware are.

Identify what the steps are that Incident Handlers should follow to handle Malware safely.

Define what the steps that the IH&R team should carry out to prepare the test system for malware analysis are.

External Resources:

Preparation for Handling Malware Incidents

What is Malware? - malicious software that damages or disables computer systems and gives control of the systems to the malware creator.

The following are types of malware:

▪ Trojan Horse - a program in which the malicious or harmful code is contained inside harmless programming or data.

▪ Backdoor - a program that can bypass the standard system authentication or conventional system mechanism like IDS and firewalls without being detected. The difference between this type of malware and other types of malware is that the installation of the backdoor is performed without the user's knowledge. This allows the attack to perform any activity on the infected computer, which can include transferring, modifying, corrupting files, installing malicious software, rebooting the machine, and so on without user detection.

▪ Rootkit - goal of the rootkit is to gain root privileges to a system; builds a backdoor login process in the operating system by which the attacker can evade the standard login process. Once the user enables root access, a rootkit may attempt to hide the traces of unauthorized access by modifying drivers or kernel modules and discarding active processes. Rootkits replace certain operating system calls and utilities with their own modified versions of those routines that in turn undermine the security of the target system by executing malicious functions. A typical rootkit comprises backdoor programs, DDoS programs, packet sniffers, log-wiping utilities, IRC bots, and others.

▪ Ransomware - a type of malware that restricts access to the computer system that it infects, or critical files and documents stored on it, and thereafter demands an online ransom payment to the malware creator(s) to remove user restrictions. Ransomware might encrypt files stored on the system's hard disk, or merely lock the system and display messages meant to trick the user into paying. Usually, ransomware spreads as a Trojan, entering a system through email attachments, hacked websites, infected programs, app downloads from untrusted sites, vulnerabilities in network services, and so on. After execution, the payload in the ransomware runs and encrypts the victim's data (files and documents), which can be decrypted only by the malware author.

▪ Adware - software used to display online advertisements in the user interface or on a screen and generate revenue. Attackers use this property of adware to display malicious advertisements that redirect users to malicious websites that collect user data without their consent or automatically download other malware.

▪ Virus - viruses can infect outside machines only with the assistance of computer users. Some viruses affect computers as soon as their code is executed; other viruses lie dormant until a pre-determined logical circumstance is met. Viruses infect a variety of files, such as overlay files (.OVL) and executable files (.EXE, .SYS, .COM, or .BAT). Viruses are transmitted through file downloads, infected disk/flash drives, and as email attachments.

▪ Worms - standalone malicious programs that replicate, execute, and spread across network connections independently, without human intervention.

▪ Spyware - stealthy computer monitoring software that allows you to secretly record all the user activities on the target computer. It automatically delivers logs to the remote attacker using internet (via email, FTP, Command and Control through encrypted traffic, HTTP, DNS, etc.).

▪ Botnet - a network of compromised systems used by attackers to perform denial-of-service (DoS) attacks. Bots are software applications that run automated tasks over the internet.

▪ Crypter - software that encrypts the original binary code of the .exe file. Attackers use crypters to hide viruses, spyware, keyloggers, Remote Access Trojans (RATs), among others, to make them undetectable by antivirus software.

What are the basic components of Malware? -

```
▪ Crypter - software that encrypts the original binary code of the .exe
file. Attackers use crypters to hide viruses, spyware, keyloggers, Remote
Access Trojans (RATs), among others, to make them undetectable by antivirus
software.

▪ Downloader - Trojan that downloads other malware from the internet onto
the PC; attackers install downloader software when they first gain access to
a system.

▪ Dropper - Trojan that installs other malware files onto the system either
from a malware package or the internet.

▪ Exploit - Malicious code that breaches system security via software
vulnerabilities to access information or install malware.

▪ Injector - A program that injects its code into other vulnerable running
processes, altering the execution of the process in order to hide or prevent
its removal.

▪ Obfuscator - A program that conceals its code and intended purpose via
various techniques, making it hard for security mechanisms to detect or
remove it.

▪ Packer - A program that allows all files to bundle together into a single
executable file via compression in order to bypass security software detection.

▪ Payload - Software that allows control over a computer system after it has
been executed.
```

What are the steps that Incident Handlers should follow to handle Malware safely? -

```
▪ Always use a virtual machine or sandbox environment for handling malware
that is FULLY isolated.
▪ Use secure channels and dedicated media for the purpose of transferring
malware files.
▪ Keep malware files zipped and password protected to avoid accidental execution.
▪ Modify the identified malware file extensions or add an invalid file
extension to malware files to ensure no application is associated with it.
▪ Store the malware files in an isolated storage facility.
```

What are the steps to prepare the test system? -

```
▪ Step 1: Allocate a physical system for the analysis lab.
▪ Step 2: Create a virtual machine on the physical system.
▪ Step 3: Install a guest OS on the virtual machine(s).
▪ Step 4: Isolate the system from the network by ensuring that the NIC card is
in “host only” mode.
▪ Step 5: Simulate internet services using tools such as iNetSim.
▪ Step 6: Disable any/all sharing capabilities for the VM.
▪ Step 7: Install malware analysis tools.
▪ Step 8: Generate hash value of each OS and tool.
▪ Step 9: Copy the malware over to the guest OS.
```