LESSON NOTES

CYBERSECURITY

Domain 2.0 - General Security Concepts

2.4.1 - Malware

Lesson Overview:

Students will:

- Analyze potential indicators to determine the type of attack.

Guiding Question: What are some common malware types?

Suggested Grade Levels: 10 - 12

CompTIA Security+ SYO-701 Objective:

2.4 - Given a scenario, analyze indicators of malicious activity

- Malware attacks

This content is based upon work supported by the US Department of Homeland Security's Cybersecurity & Infrastructure Security Agency under the Cybersecurity Education Training and Assistance Program (CETAP).

Malware

Malware is the generic term applied to software that is utilized for malicious purposes. That is not to say that malware cannot be employed for other means, but in the context of cyber security, any software utilized to subvert the confidentiality, integrity, or availability of information and the systems that process them is referred to as malware.

Types of Malware

Malware can be used to refer to the following software:
Viruses, worms, and sometimes trojans are used interchangeably; however, viruses are the larger family of malware that refers to any piece of code that attaches itself to system processes, files, or programs. Viruses enact their intended effects using these internal programs and files as carriers. They are not able to self-replicate.

Cryptomalware is any software that uses cryptography as its intended effects. The malware utilizes CPU cycles to generate encryption keys and encrypt information on systems.

Ransomware is a form of cryptomalware that holds the target's information for ransom after encrypting it. Not all cryptomalware is ransomware, some cryptomalware can be used to create a denial of service with no promise of returning the target's access to the information.

Trojan is named after the Trojan Horse from Greek mythology wherein a large wooden horse with soldiers in its cavity was utilized to subvert the enemy's defenses. Similarly, trojan malware seeks to subvert system defenses by utilizing programs and credentials that are authorized to operate in the target's environment.

Worm is a virus that is capable of self-replicating. It does not have to rely on programs to spread.

Spyware is software that listens to user activity. An application on your phone that records your location or voice without your permission is an example of spyware.

Bloatware is applications that come preloaded on your device. These applications can be used to make money or promote a company's products. Usually, these applications make your device slower and take up space. You can remove the bloatware from your device by uninstalling or deleting it, but occasionally it can be difficult or even impossible to remove.

Keylogger is a type of malware that listens and records user's keystrokes to glean information.

Bots refers to compromised systems that act on actions typically sent from a Command and Control (C2) server. The identifying features are the autonomous and usually remote nature of the attack. A collection of bots is referred to as a botnet.

RAT (Remote Access Trojans) provide access to your device remotely.

Logic Bombs are a type of malware that relies on a specific logical sequence to trigger its effects. For example, a piece of malware will only run once it scans the environment and finds a specific PLC (programmable logic controller) by a specific maker. (This was the basis of the Stuxnet worm)

Rootkit is malware utilized to gain administrative credentials on a system. This allows the attacker to gain access to regions of the system that are otherwise off limits to non-administrative/privileged users.

Backdoor is an example of how the software alone is not malicious, although its use case is. Backdoors are commonly found in programming environments and are used to test code without having to scour the entire program or access it how a user would. It helps cut down on development time. However, a backdoor subverts other authentication mechanisms for that software thereby allowing unauthorized access.

Summary

There is a myriad of software written to subvert traditional operations of systems. Not all are utilized with an intent to harm; however, when they do, they are referred to as malware. The various types mentioned above are typically employed in concert to enact various effects against a system. Robust software development practices, employee training, regular backups, and patching and defense in depth can help mitigate the effects of malware.