Instructor Materials
Chapter 3: Cybersecurity Threats, Vulnerabilities, and Attacks

Cybersecurity Essentials v1.1

Cisco | Networking Academy®
Mind Wide Open™

Chapter 3: Cybersecurity Threats, Vulnerabilities, and Attacks

Cybersecurity Essentials v1.1

Cisco | Networking Academy®
Mind Wide Open™

Chapter 3 - Sections & Objectives

3.1 Malware and Malicious Code

Differentiate the types of malware and malicious code.

3.2 Deception

Describe the tactics, techniques and procedures used by cyber criminals.

3.3 Attacks

Compare the different methods used in social engineering.

Compare different types of cyberattacks.

3.1 Malware and Malicious Code

Cisco | Networking Academy®
Mind Wide Open™

Malware and Malicious Code

Types of Malware

Cyber criminals target user’s end devices through the installation of malware.

Viruses - A virus is malicious executable code attached to another executable file, such as a legitimate program. Most viruses require end-user initiation, and can activate at a specific time or date.

Worms - Worms are malicious code that replicates by independently exploiting vulnerabilities in networks. Worms usually slow down networks. Whereas a virus requires a host program to run, worms can run by themselves. Other than the initial infection, worms no longer require user participation.

Trojan horse - A Trojan horse is malware that carries out malicious operations under the guise of a desired operation such as playing an online game. This malicious code exploits the privileges of the user that runs it. A Trojan horse differs from a virus because the Trojan binds itself to non-executable files, such as image files, audio files, or games.

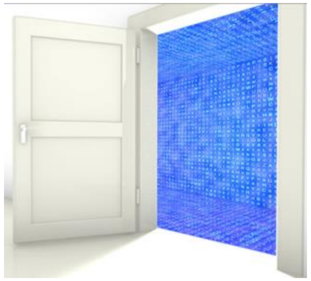
Malware and Malicious Code

Types of Malware (Cont.)

- **Logic Bomb** - A logic bomb is a malicious program that uses a trigger to awaken the malicious code. For example, triggers can be dates, times, other programs running, or the deletion of a user account. The logic bomb remains inactive until that trigger event happens. Once activated, a logic bomb implements a malicious code that causes harm to a computer.

- **Ransomware** - Ransomware holds a computer system, or the data it contains, captive until the target makes a payment. Ransomware usually works by encrypting data in the computer with a key unknown to the user.

- **Backdoors and Rootkits** - A backdoor or rootkit refers to the program or code introduced by a criminal who has compromised a system. The backdoor bypasses the normal authentication used to access a system. A rootkit modifies the operating system to create a backdoor. Attackers then use the backdoor to access the computer remotely.



Malware and Malicious Code

Email and Browser Attacks (Cont.)

Email is a universal service used by billions worldwide. As one of the most popular services, email has become a major vulnerability to users and organizations.

Spam - Spam, also known as junk mail, is unsolicited email. In most cases, spam is a method of advertising. However, spam can send harmful links, malware, or deceptive content.

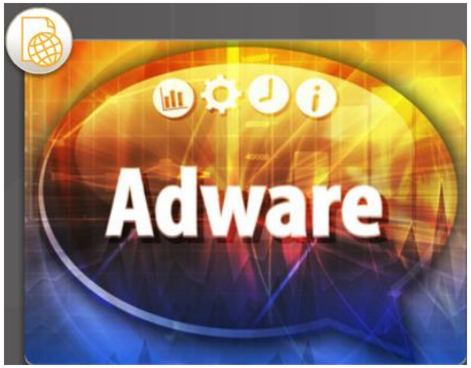
Spyware - Spyware is software that enables a criminal to obtain information about a user’s computer activities. Spyware often includes activity trackers, keystroke collection, and data capture. In an attempt to overcome security measures, spyware often modifies security settings.

Malware and Malicious Code

Email and Browser Attacks (Cont.)

Adware - Adware typically displays annoying pop-ups to generate revenue for its authors. The malware may analyze user interests by tracking the websites visited. It can then send pop-up advertising pertinent to those sites.

Scareware - Scareware persuades the user to take a specific action based on fear. Scareware forges pop-up windows that resemble operating system dialogue windows.



Malware and Malicious Code

Email and Browser Attacks (Cont.)

Phishing - Phishing is a form of fraud. Cyber criminals use email, instant messaging, or other social media to try to gather information such as login credentials or account information by masquerading as a reputable entity or person. Phishing occurs when a malicious party sends a fraudulent email disguised as being from a legitimate, trusted source. The message intent is to trick the recipient into installing malware on his or her device or into sharing personal or financial information.

Spear phishing - Spear phishing is a highly targeted phishing attack. While phishing and spear phishing both use emails to reach the victims, spear phishing sends customized emails to a specific person.

Malware and Malicious Code

Email and Browser Attacks (Cont.)

Vishing - Vishing is phishing using voice communication technology. Criminals can spoof calls from legitimate sources using voice over IP (VoIP) technology. Victims may also receive a recorded message that appears legitimate.

Pharming - Pharming is the impersonation of a legitimate website in an effort to deceive users into entering their credentials.

Whaling - Whaling is a phishing attack that targets high profile targets within an organization such as senior executives.

Malware and Malicious Code

Email and Browser Attacks (Cont.)

Plugins - The Flash and Shockwave plugins from Adobe enable the development of interesting graphic and cartoon animations that greatly enhance the look and feel of a web page. Plugins display the content developed using the appropriate software.

SEO Poisoning - Search engines such as Google work by ranking pages and presenting relevant results based on users' search queries. Depending on the relevancy of web site content, it may appear higher or lower in the search result list. SEO, short for Search Engine Optimization, is a set of techniques used to improve a website's ranking by a search engine. While many legitimate companies specialize in optimizing websites to better position them, SEO poisoning uses SEO to make a malicious website appear higher in search results.

Browser Hijacker - A browser hijacker is malware that alters a computer's browser settings to redirect the user to websites paid for by the cyber criminals' customers. Browser hijackers usually install without the user's permission and is usually part of a drive-by download.

3.2 Deception

Cisco | Networking Academy®
Mind Wide Open™

Deception

The Art of Deception

Social Engineering - Social engineering is a completely non-technical means for a criminal to gather information on a target. Social engineering is an attack that attempts to manipulate individuals into performing actions or divulging confidential information.

Social engineers often rely on people's willingness to be helpful but also prey on people's weaknesses. These are some types of social engineering attacks:

Pretexting - This is when an attacker calls an individual and lies to them in an attempt to gain access to privileged data. An example involves an attacker who pretends to need personal or financial data in order to confirm the identity of the recipient.

Something for Something (Quid pro quo) - This is when an attacker requests personal information from a party in exchange for something, like a gift.

Hi this is Amy from the help desk. We need to upgrade the software on your computer after work hours. What is your user ID and password? You can change the password tomorrow when you log in.
Social Engineer

Ok, my user ID and password are...
Unsuspecting Employee at XYZ Corporation

Deception

Types of Deception

Shoulder Surfing and Dumpster Diving – refers to picking up PINs, access codes or credit card numbers. An attacker can be in close proximity to his victim or the attacker can use binoculars or closed circuit cameras to shoulder surf.

Impersonation and Hoaxes - Impersonation is the action of pretending to be someone else. For example, a recent phone scam targeted taxpayers. A criminal, posing as an IRS employee, told the victims that they owed money to the IRS.

Piggybacking and Tailgating - Piggybacking occurs when a criminal tags along with an authorized person to gain entry into a secure location or a restricted area. Tailgating is another term that describes the same practice.

Online, Email, and Web-based Trickery - Forwarding hoax emails and other jokes, funny movies, and non-work-related emails at work may violate the company's acceptable use policy and result in disciplinary actions.

3.3 Attacks

Cisco | Networking Academy®
Mind Wide Open™

Attacks

Types of Cyber Attacks

Denial-of-Service (DoS) Attacks - are a type of network attack. A DoS attack results in some sort of interruption of network services to users, devices, or applications. DoS attacks are a major risk because they can easily interrupt communication and cause significant loss of time and money. These attacks are relatively simple to conduct, even by an unskilled attacker.

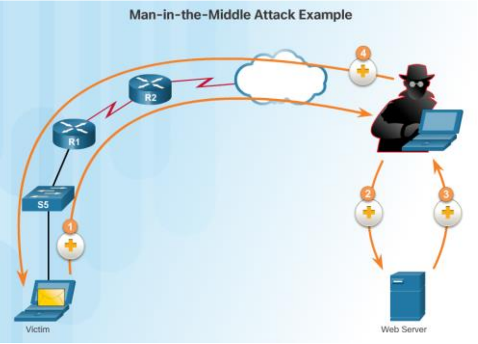
Sniffing - Sniffing is similar to eavesdropping on someone. It occurs when attackers examine all network traffic as it passes through their NIC, independent of whether or not the traffic is addressed to them or not. Criminals accomplish network sniffing with a software application, hardware device, or a combination of the two.

Spoofing - Spoofing is an impersonation attack, and it takes advantage of a trusted relationship between two systems. If two systems accept the authentication accomplished by each other, an individual logged onto one system might not go through an authentication process again to access the other system.

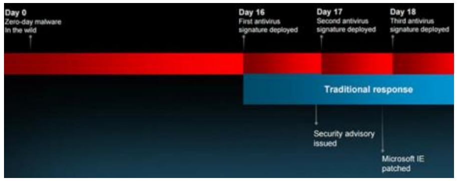
Attacks

Types of Cyber Attacks

Man-in-the-middle - A criminal performs a man-in-the-middle (MitM) attack by intercepting communications between computers to steal information crossing the network. The criminal can also choose to manipulate messages and relay false information between hosts since the hosts are unaware that a modification to the messages occurred. MitM allows the criminal to take control over a device without the user’s knowledge.



Zero-Day Attacks - A zero-day attack, sometimes referred to as a zero-day threat, is a computer attack that tries to exploit software vulnerabilities that are unknown or undisclosed by the software vendor. The term zero hour describes the moment when someone discovers the exploit.


Day 0
Zero-day malware in the wild
Day 16
First antivirus signature deployed
Day 17
Second antivirus signature deployed
Day 18
Third antivirus signature deployed
Traditional response
Security advisory issued
Microsoft IE patched

Keyboard Logging - Keyboard logging is a software program that records or logs the keystrokes of the user of the system. Criminals can implement keystroke loggers through software installed on a computer system or through hardware physically attached to a computer. The criminal configures the key logger software to email the log file. The keystrokes captured in the log file can reveal usernames, passwords, websites visited, and other sensitive information.

Attacks

Wireless and Mobile Attacks (Cont.)

Grayware and SMiShing

- Grayware includes applications that behave in an annoying or undesirable manner. Grayware may not have recognizable malware concealed within, but it still may pose a risk to the user. Grayware is becoming a problem area in mobile security with the popularity of smartphones.
- SMiShing is short for SMS phishing. It uses Short Message Service (SMS) to send fake text messages. The criminals trick the user into visiting a website or calling a phone number. Unsuspecting victims may then provide sensitive information such as credit card information. Visiting a website might result in the user unknowingly downloading malware that infects the device.

Wireless and Mobile Attacks (Cont.)

Rogue Access Points - A rogue access point is a wireless access point installed on a secure network without explicit authorization. A rogue access point can be set up in two ways.

RF Jamming - Wireless signals are susceptible to electromagnetic interference (EMI), radio-frequency interference (RFI), and may even be susceptible to lightning strikes or noise from fluorescent lights. Wireless signals are also susceptible to deliberate jamming. Radio frequency (RF) jamming disrupts the transmission of a radio or satellite station so that the signal does not reach the receiving station.

Bluejacking and Bluesnarfing - Bluejacking is the term used for sending unauthorized messages to another Bluetooth device. Bluesnarfing occurs when the attacker copies the victim's information from his device. This information can include emails and contact lists.

Attacks

Wireless and Mobile Attacks (Cont.)

WEP and WPA Attacks

Wired Equivalent Privacy (WEP) is a security protocol that attempted to provide a wireless local area network (WLAN) with the same level of security as a wired LAN. Since physical security measures help to protect a wired LAN, WEP seeks to provide similar protection for data transmitted over the WLAN with encryption.

- WEP uses a key for encryption.
- There is no provision for key management with WEP, so the number of people sharing the key will continually grow.

Wi-Fi Protected Access (WPA) and then WPA2 came out as improved protocols to replace WEP. WPA2 does not have the same encryption problems because an attacker cannot recover the key by observing traffic.

- WPA2 is susceptible to attack because cyber criminals can analyze the packets going between the access point and a legitimate user.
- Cyber criminals use a packet sniffer and then run attacks offline on the passphrase.

Attacks

Wireless and Mobile Attacks (Cont.)

Defending Against Wireless and Mobile Device Attacks

There are several steps to take to defend against wireless and mobile device attacks.

- Most WLAN products use default settings. Take advantage of the basic wireless security features such as authentication and encryption by changing the default configuration settings.
- Restrict access point placement with the network by placing these devices outside the firewall or within a demilitarized zone (DMZ) which contains other untrusted devices such as email and web servers.
- WLAN tools such as NetStumbler may discover rogue access points or unauthorized workstations. Develop a guest policy to address the need when legitimate guests need to connect to the Internet while visiting. For authorized employees, utilize a remote access virtual private network (VPN) for WLAN access.

Attacks

Application Attacks

Cross-site scripting (XSS) - is a vulnerability found in web applications. XSS allows criminals to inject scripts into the web pages viewed by users. This script can contain malicious code. Cross-site scripting has three participants: the criminal, the victim, and the website. The cyber-criminal does not target a victim directly. The criminal exploits vulnerability within a website or web application. Criminals inject client-side scripts into web pages viewed by users, the victims.

Code Injections Attacks - One way to store data at a website is to use a database. There are several different types of databases such as a Structured Query Language (SQL) database or an Extensible Markup Language (XML) database. Both XML and SQL injection attacks exploit weaknesses in the program such as not validating database queries properly.

Buffer Overflow - A buffer overflow occurs when data goes beyond the limits of a buffer. Buffers are memory areas allocated to an application. By changing data beyond the boundaries of a buffer, the application accesses memory allocated to other processes. This can lead to a system crash, data compromise, or provide escalation of privileges.

Attacks

Application Attacks

Remote Code Executions vulnerabilities allow a cybercriminal to execute malicious code and take control of a system with the privileges of the user running the application. Remote code execution allows a criminal to execute any command on a target machine.

ActiveX Controls and Java controls provide the capability of a plugin to Internet Explorer.

- ActiveX controls are pieces of software installed by users to provide extended capabilities. Third parties write some ActiveX controls and they may be malicious. They can monitor browsing habits, install malware, or log keystrokes. Active X controls also work in other Microsoft applications.
- Java operates through an interpreter, the Java Virtual Machine (JVM). The JVM enables the Java program’s functionality. The JVM sandboxes or isolates untrusted code from the rest of the operating system. There are vulnerabilities, which allow untrusted code to go around the restrictions imposed by the sandbox.

Attacks

Application Attacks

Defending Against Application Attacks

- The first line of defense against an application attack is to write solid code.
- Regardless of the language used, or the source of outside input, prudent programming practice is to treat all input from outside a function as hostile.
- Validate all inputs as if they were hostile.
- Keep all software including operating systems and applications up to date, and do not ignore update prompts.
- Not all programs update automatically, so at the very least, always select the manual update option.

3.4 Chapter Summary

Cisco | Networking Academy®
Mind Wide Open™

Chapter Summary

Summary

Threats, vulnerabilities, and attacks are the central focus of the cybersecurity specialists.

- This chapter discussed the various cybersecurity attacks that cyber criminals launch.
- The chapter explained the threat of malware and malicious code.
- The chapter discussed the types of deception involved with social engineering. Maneuvering explained the types of attacks that both wired and wireless networks experience.
- Finally, the chapter discussed the vulnerabilities presented by application attacks.

Understanding the types of possible threats allows an organization to identify the vulnerabilities that make it a target. The organization can then learn how to defend itself against cybersecurity trickery and maneuvering.

Cisco | Networking Academy®

Mind Wide Open™