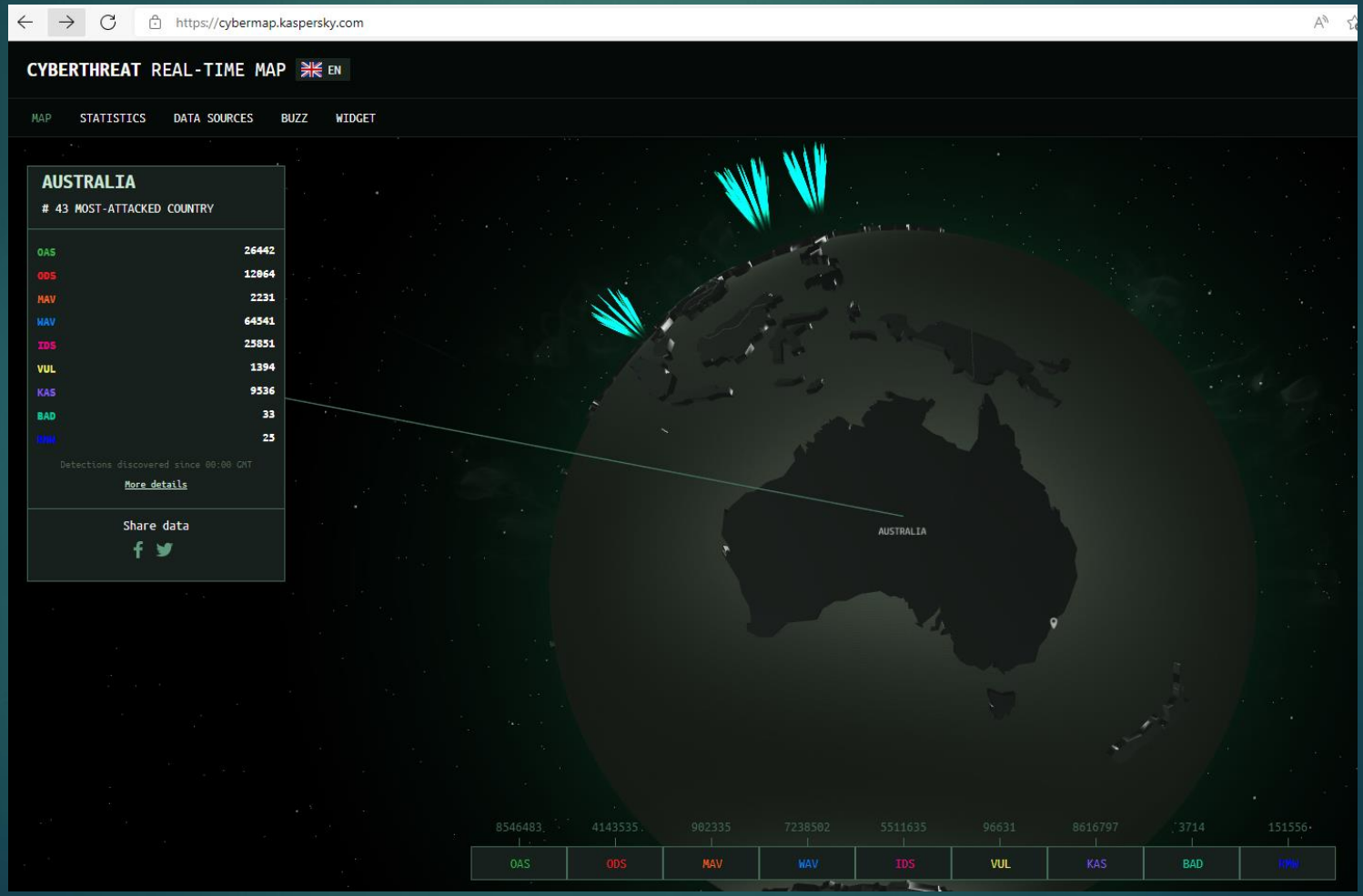
Module 1: Cybersecurity - A World of Experts and Criminals

Objectives

- Describe the common characteristics comprising the cybersecurity world
- Differentiate the characteristics of cyber criminals and cybersecurity specialists
- Compare how cybersecurity threats affect individuals, businesses, and organizations
- Analyze the factors that lead to the spread and growth of cybercrime
- Analyze the organizations and efforts committed to expanding the cybersecurity workforce
- Differentiate the types of malware and malicious code.
- Describe the tactics, techniques and procedures used by cyber criminals.

Networks Are Targets

https://cybermap.kaspersky.com/



The Cybersecurity World

Cybersecurity Domains

- Websites and Power of Data
  - Great businesses have been created by collecting and harnessing the power of data and data analytics
  - These businesses have the responsibility to protect this data from misuse and unauthorized access
  - The growth of data has created great opportunities for cybersecurity specialists
- Domains
  - Business large and small have recognized the power of big data and data analytics
  - Organizations like Google, LinkedIn, Amazon provide important services and opportunity for their customers
  - The growth in data collection and analytics poses great risks to individuals and modern life if precautions are not taken to protect sensitive data from criminals or others who have intent to harm

Cybersecurity Criminals vs Cybersecurity Specialists

Cybersecurity Criminals

- **Hackers** – This group of criminals breaks into computers or networks to gain access for various reasons.
  - ***White hat*** attackers break into networks or computer systems to discover weaknesses in order to improve the security of these systems.
  - ***Gray hat*** attackers are somewhere between white and black hat attackers. The gray hat attackers may find a vulnerability and report it to the owners of the system if that action coincides with their agenda.
  - ***Black hat*** attackers are unethical criminals who violate computer and network security for personal gain, or for malicious reasons, such as attacking networks.

Activity – Identify Hat Colour

Hacker Characteristic	White Hat	Gray Hat	Black Hat
After hacking into ATM machines remotely using a laptop, he worked with ATM manufacturers to resolve the found security vulnerabilities.			
From my laptop, I transferred $10 million to my bank account using victim account numbers and PINs after viewing recordings of victims entering the numbers.			
My job is to identify weaknesses in the computer system in my company.			
I used malware to compromise several corporate system to steal credit card information and sold that information to the highest bidder.			
During my research for security exploits, I stumbled across a security vulnerability on a corporate network that I am authorized to access.			
I am working with technology companies to fix a flaw with DNS.			

Cybersecurity Criminals (Cont.)

Criminals come in many different forms. Each have their own motives:

- **Script Kiddies** - Teenagers or hobbyists mostly limited to pranks and vandalism, have little or no skill, often using existing tools or instructions found on the Internet to launch attacks.
- **Vulnerability Brokers** - Grey hat hackers who attempt to discover exploits and report them to vendors, sometimes for prizes or rewards.
- **Hacktivists -** Grey hat hackers who rally and protest against different political and social ideas. Hacktivists publicly protest against organizations or governments by posting articles, videos, leaking sensitive information, and performing distributed denial of service (DDoS) attacks.

Cybersecurity Criminals (Cont.)

- **Cyber Criminals** - These are black hat hackers who are either self-employed or working for large cybercrime organizations. Each year, cyber criminals are responsible for stealing billions of dollars from consumers and businesses.
- **State Sponsored Hackers -** Depending on a person's perspective, these are either white hat or black hat hackers who steal government secrets, gather intelligence, and sabotage networks. Their targets are foreign governments, terrorist groups, and corporations.

Cybersecurity Criminals vs Cybersecurity Specialists

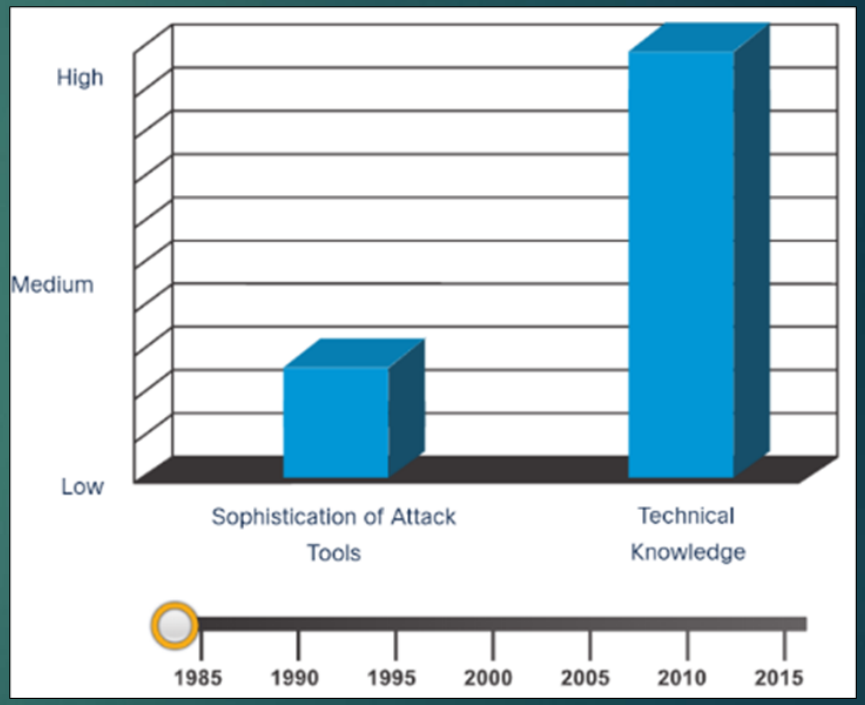
Evolution of Threat Actors

- Hacking started in the 1960s with phone freaking, which refers to using various audio frequencies to manipulate phone systems.
- In the early 1960's, threat actors realized that by mimicking a tone using a whistle, they could exploit the phone switches to make free long-distance calls.
- In the mid-1980's, threat actors wrote 'war dialing' programs which dialed each telephone number in a given area in search of computers, bulletin board systems, and fax machines.
- When a phone number was found, password-cracking programs were used to gain access.

Cybersecurity Criminals vs Cybersecurity Specialists

Introduction of Attack Tools

- To exploit vulnerability, a threat actor must have a technique or tool.
- Over the years, attack tools have become more sophisticated, and highly automated.
- These new tools require less technical knowledge to implement.



Introduction of Attack Tools

- Ethical hacking involves using many different types of tools to test the network and end devices.
- To validate the security of a network and its systems, many network penetration testing tools have been developed and many of these tools can also be used by threat actors for exploitation.
- Threat actors have also created various hacking tools. Cybersecurity personnel must also know how to use these tools when performing network penetration tests.
- **Note:** Most of these tools are UNIX or Linux based; therefore, a security professional should have a strong UNIX and Linux background.

Cybersecurity Criminals vs Cybersecurity Specialists

Introduction of Attack Tools

- The following table lists some of the categories of common network penetration testing tools.

Categories of Tools	Description
Password crackers	Used to crack or recover the password. Eg:John the Ripper, Ophcrack
Wireless hacking tools	Used to intentionally hack into a wireless network to detect security vulnerabilities. Eg:Aircrack-ng, Kismet
Network scanning and hacking tools	Used to probe network devices, servers, and hosts for open TCP or UDP ports. Eg: Nmap, SuperScan
Packet crafting tools	Used to probe and test a firewall's robustness. Eg: Hping, Scapy
Packet sniffers	Used to capture and analyze packets within traditional Ethernet LANs or WLANs. Eg: Wireshark, Tcpdump
Rootkit detectors	It is a directory and file integrity checker used by white hats to detect installed root kits. Eg: AIDE, Netfilter
Fuzzers to search vulnerabilities	Used by threat actors when attempting to discover a computer system's security vulnerabilities. Eg: Skipfish, Wapiti

Cybersecurity Criminals vs Cybersecurity Specialists

Introduction of Attack Tools

Categories of Tools	Description
Forensic tools	White hat hackers use these tools to sniff out any trace of evidence existing in a particular computer system. Eg: Sleuth Kit, Helix
Debuggers	Used by black hats to reverse engineer binary files when writing exploits and used by white hats when analyzing malware. Eg:GDB, WinDbg
Hacking operating systems	These are preloaded with tools and technologies optimized for hacking. Eg: Kali Linux, SELinux
Encryption tools	These tools use algorithm schemes to encode the data to prevent unauthorized access to the data. Eg: VeraCrypt, CipherShed
Vulnerability exploitation tools	These tools identify whether a remote host is vulnerable to a security attack. Eg: Metasploit, Core Impact
Vulnerability scanners	These tools scan a network or system to identify open ports. They can also be used to scan for known vulnerabilities and scan VMs, BYOD devices, and client databases. Eg:Nipper, Securia PSI

Cybersecurity Criminals vs Cybersecurity Specialists

Threat, Vulnerability, and Risk

- To understand network security, it is important to know the following terms:

TERM	EXPLANATION
Threat	A potential danger to an asset such as data or the network itself.
Vulnerability	A weakness in a system or its design that could be exploited by a threat.
Attack Surface	An attack surface is the total sum of the vulnerabilities in a given system that are accessible to an attacker. The attack surface describes different points where an attacker could get into a system, and where they could get data out of the system.
Exploit	The mechanism that is used to leverage a vulnerability to compromise an asset. Exploits may be remote or local. A remote exploit is one that works over the network without any prior access to the target system. In a local exploit, the threat actor has some type of user or administrative access to the end system. It does not necessarily mean that the attacker has physical access to the end system.
Risk	The likelihood that a particular threat will exploit a particular vulnerability of an asset and result in an undesirable consequence.

Threat, Vulnerability, and Risk (Contd.)

- **Common network security terms:**
  - Countermeasure – Actions taken to protect assets by mitigating a threat or reducing risk.
  - Impact - The potential damage to the organization that is caused by the threat
- **Note:** A local exploit requires inside network access such as a user with an account on the network. It does not require an account on the network to exploit that network's vulnerability.

Cybersecurity Criminals vs Cybersecurity Specialists

Cybersecurity Tasks

- Threat actors target the home users, small-to-medium sized businesses, as well as large public and private organizations.
- Hence, Cybersecurity is a shared responsibility which all users must practice to make the internet and networks safer and more secure.
- Organizations must take action and protect their assets, users, and customers. They must develop and practice cybersecurity tasks such as those mentioned in the figure.

Cybersecurity Criminals vs Cybersecurity Specialists

Threat Sharing and Building Cybersecurity Awareness

- Governments are now actively promoting cybersecurity.
- The US Cybersecurity Infrastructure and Security Agency (CISA) is leading efforts to automate the sharing of cybersecurity information with public and private organizations at no cost.
- CISA use a system called Automated Indicator Sharing (AIS) which enables the sharing of attack indicators between the US government and the private sector as soon as threats are verified.
- The European Union Agency for Cybersecurity (ENISA) delivers advice and solutions for the cybersecurity challenges of the EU member states.
- The CISA and the National Cyber Security Alliance (NCSA) have an annual campaign in every October called National Cybersecurity Awareness Month (NCASM) to raise awareness about cybersecurity.

Cybersecurity Criminals versus Cybersecurity Specialists

Cybersecurity Specialists

Thwarting the cyber criminals is a difficult task, company, government and international organizations have begun to take coordinated actions to limit or fend off cyber criminals. The coordinated actions include:

- **Vulnerability Database**: The Nation Common Vulnerabilities and Exposures (CVE) database is an example of the development of a national database. The CVE National Database was developed to provide a publicly available database of all know vulnerabilities. http://www.cvedetails.com/
- **Early Warning Systems**: The Honeynet project is an example of creating Early Warning Systems. The project provides a HoneyMap which displays real-time visualization of attacks. https://www.honeynet.org/node/960
- **Share Cyber Intelligence**: InfraGard is an example of wide spread sharing of cyber intelligence. The InfraGard program is a partnership between the FBI and the private sector. The participants are dedicated to sharing information and intelligence to prevent hostile cyberattacks. https://www.infragard.org/

Cybersecurity Specialists (Cont.)

- **ISM Standards**: The ISO 27000 standards are an example of Information Security Management Standards. The standards provide a framework for implementing cybersecurity measures within an organization. http://www.27000.org/
- **New Laws**: The ISACA group track law enacted related to cyber security. These laws can address individual privacy to protection of intellectual property. Examples of these laws include: Cybersecurity Act, Federal Exchange Data Breach Notification Act and the Data Accountability and Trust Act. http://www.isaca.org/cyber/pages/cybersecuritylegislation.aspx

Activity – Identify Cybersecurity Countermeasure used to Thwart Cyber Criminal

- New Laws
- ISM Standards
- Early Warning Systems
- Vulnerability Database
- Sharing Intelligence

Term	Description
	The Honeynet Project
	The InfraGard program
	ISO/IEC 27000
	Cybersecurity Act
	The Nation Common Vulnerabilities and Exposures (CVE) project

Threat Arenas

Common Threats to End Users

The following examples are just a few sources of data that can come from established organizations:

Threat Arenas

Threat to Internet Services

Network services like DNS, HTTP and Online Databases are prime targets for cyber criminals.

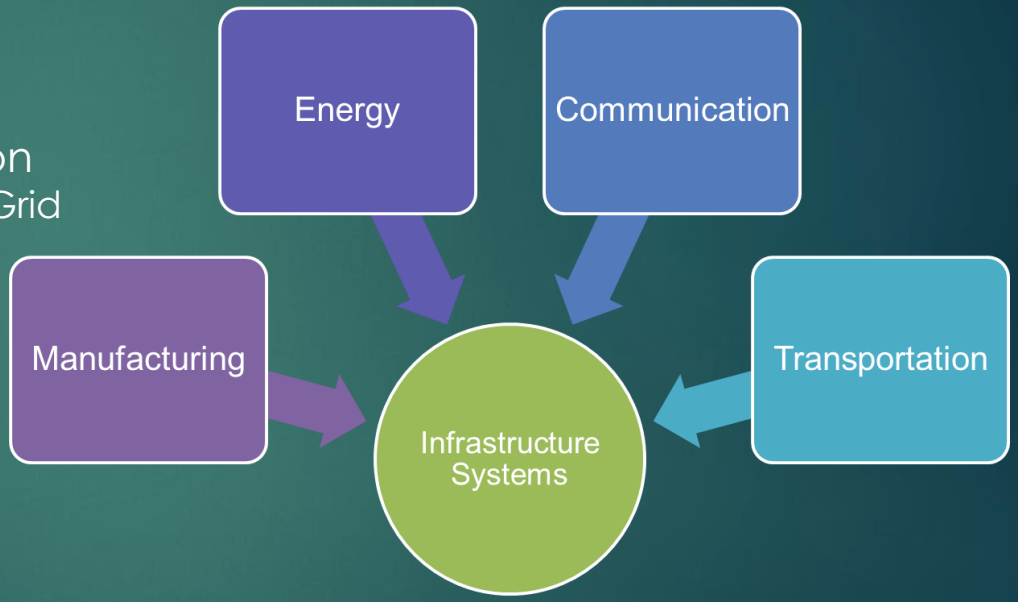
- Criminals use packet-sniffing tools to capture data streams over a network. Packet sniffers work by monitoring and recording all information coming across a network.
- Criminals can also use rogue devices, such as unsecured Wi-Fi access points.
- Packet forgery (or packet injection) interferes with an established network communication by constructing packets to appear as if they are part of a communication.

Threat Arenas

Threat To Key Industry Sectors

Domains include:

- Manufacturing
  - Industry Controls
  - Automation
  - SCADA
- Energy Production and Distribution
  - Electrical Distribution and Smart Grid
  - Oil and Gas
- Communication
  - Phone
  - Email
  - Messaging
- Transportation systems
  - Air Travel
  - Rail
  - Over the Road



Stuxnet

Threat Arenas

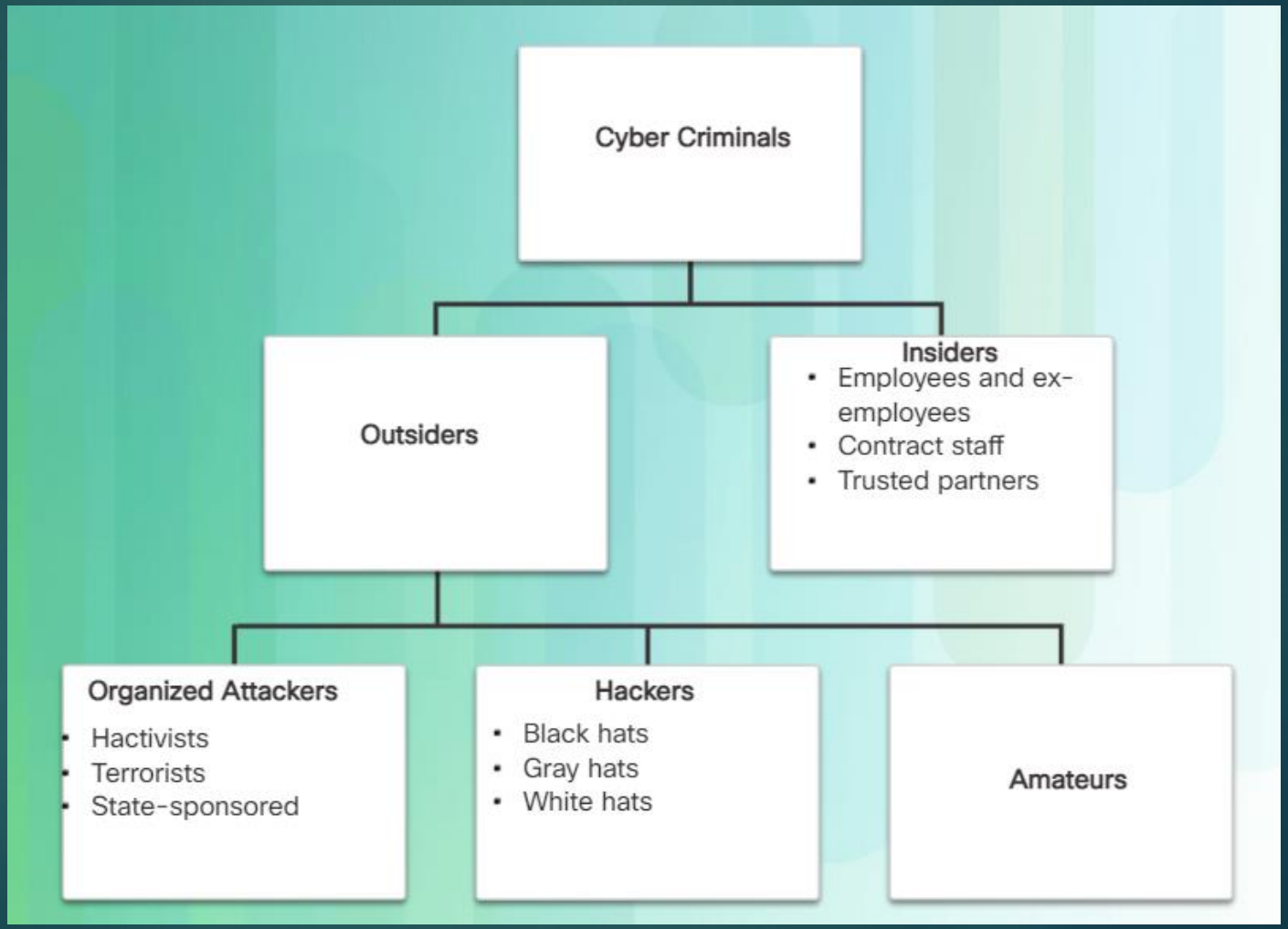
Threats to People's Way of Life

- On a personal level, everyone needs to safeguard his or her identity, data, and computing devices.
- At the corporate level, it is the employees' responsibility to protect the organization's reputation, data, and customers.
- At the state level, national security and the citizens' safety and well-being are at stake.
- The Australian Security Intelligence Organisation (ASIO) is an Australian intelligence agency and the nation's security service, ASIO protects Australia and Australians from threats to their security.

Spreading Cybersecurity Threats

How Threats Spread

Attacks can originate from within an organization or from outside of the organization.



Spreading Cybersecurity Threats

How Threats Spread (Cont.)

Vulnerabilities of Mobile Devices - The inability to centrally manage and update mobile devices poses a growing threat to organizations that allow employee mobile devices on their networks.

Spreading Cybersecurity Threats

How Threats Spread (Cont.)

- **Emergence Internet-of-Things** - The Internet of Things (IoT) is the collection of technologies that enable the connection of various devices to the Internet.

Spreading Cybersecurity Threats

How Threats Spread (Cont.)

Impact of Big Data – Big data is the result of data sets that are large and complex, making traditional data processing applications inadequate. Big data poses both challenges and opportunities based on three dimensions:

- The volume or amount of data
- The velocity or speed of data
- The variety or range of data types and sources

Creating More Experts

Online Cybersecurity Communities

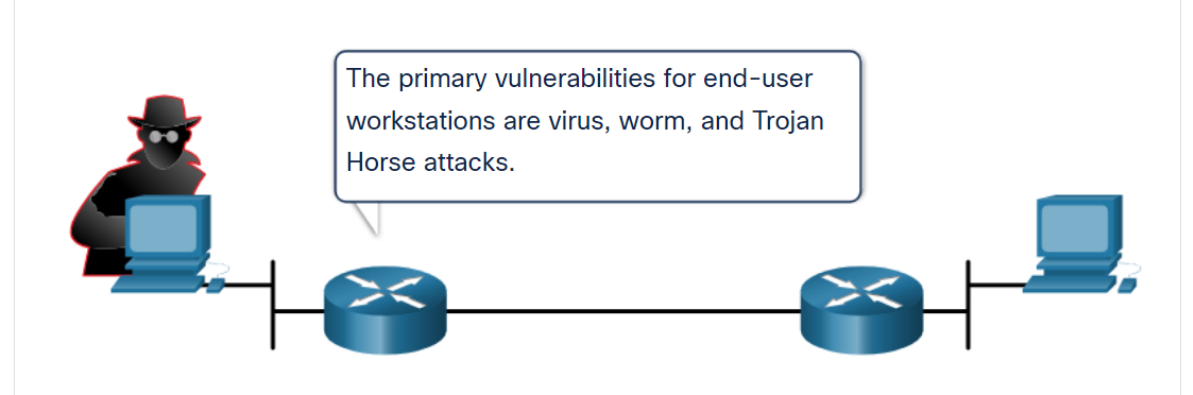
Professional Organizations

- Cybersecurity specialists must collaborate with professional colleagues frequently. International technology organizations often sponsor workshops and conferences. Visit each site with your class and explore the resources available.

Common Threats and Attacks

Types of Malware

- Malware is a code or software designed to damage, disrupt, steal, or inflict some other 'bad' or illegitimate action on data, hosts, or networks.
- The three most common types of malware are Virus, Worm, and Trojan horse.



Common Threats and Attacks

Viruses

- A virus is a type of malware that spreads by inserting a copy of itself into another program.
- After the program is run, viruses spread from one computer to another, thus infecting the computers.
- A simple virus may install itself at the first line of code in an executable file.
- Viruses can be harmless, for those that display a picture on the screen, or they can be destructive. They can also modify or delete files on the hard drive.
- Most viruses spread by USB memory drives, CDs, DVDs, network shares, and email. Email viruses are a common type of virus.

Common Threats and Attacks

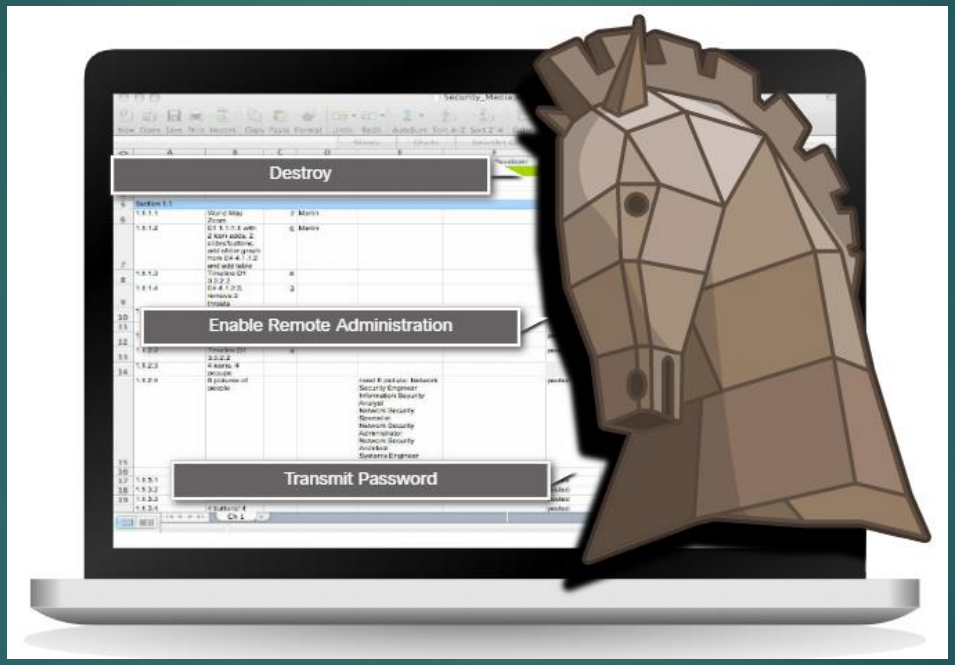
Trojan Horses

- Trojan horse malware is a software that appears to be legitimate, but it contains malicious code which exploits the privileges of the user that runs it.
- Trojans are found attached to online games.
- Users are commonly tricked into loading and executing the Trojan horse on their systems
- The Trojan horse concept is flexible.
- It can cause immediate damage, provide remote access to the system, or access through a back door.
- Custom-written Trojan horses with a specific target are difficult to detect.

Common Threats and Attacks

Trojan Horses Classification

- Trojan horses are usually classified according to the damage that they cause, or the manner in which they breach a system.



Trojan Horses Classification (Contd.)

The types of Trojan horses are as follows:

Type of Trojan Horse	Description
Remote-access	Enables unauthorized remote access.
Data-sending	Provides the threat actor with sensitive data, such as passwords.
Destructive	Corrupts or deletes files.
Proxy	Uses the victim's computer as the source device to launch attacks and perform other illegal activities.
FTP	Enables unauthorized file transfer services on end devices.
Security software disabler	Stops antivirus programs or firewalls from functioning.
Denial of Service (DoS)	Slows or halts network activity.
Keylogger	Actively attempts to steal confidential information, such as credit card numbers, by recording keystrokes entered into a web form.

Common Threats and Attacks

Worms

- Computer worms are similar to viruses because they replicate themselves by independently exploiting vulnerabilities in networks.
- Worms can slow down networks as they spread from system to system.
- Worms can run without a host program.
- However, once the host is infected, the worm spreads rapidly over the network.
- In 2001, the Code Red worm had initially infected 658 servers. Within 19 hours, the worm had infected over 300,000 servers.

Initial Code Red Worm Infection

Code Red Infection 19 hours later

Common Threats and Attacks

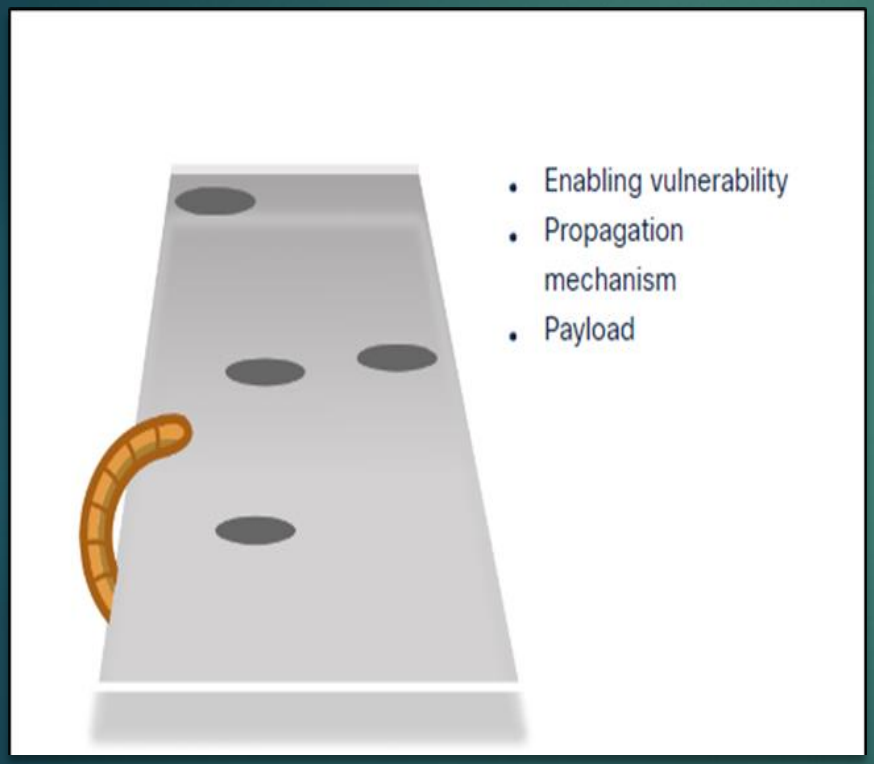
Worms (Contd.)

- The initial infection of the SQL Slammer worm is known as the worm that ate the internet.
- SQL Slammer was a Denial of Service (DoS) attack that exploited a buffer overflow bug in Microsoft's SQL Server.
- The number of infected servers doubled in size every 8.5 seconds.
- The infected servers did not have the updated patch that was released 6 months earlier.
- Hence it is essential for organizations to implement a security policy requiring updates and patches to be applied in a timely fashion.

Initial SQL Slammer Infection

SQL Slammer Infection 30 minutes later

Common Threats and Attacks
Worm Components (Contd.)

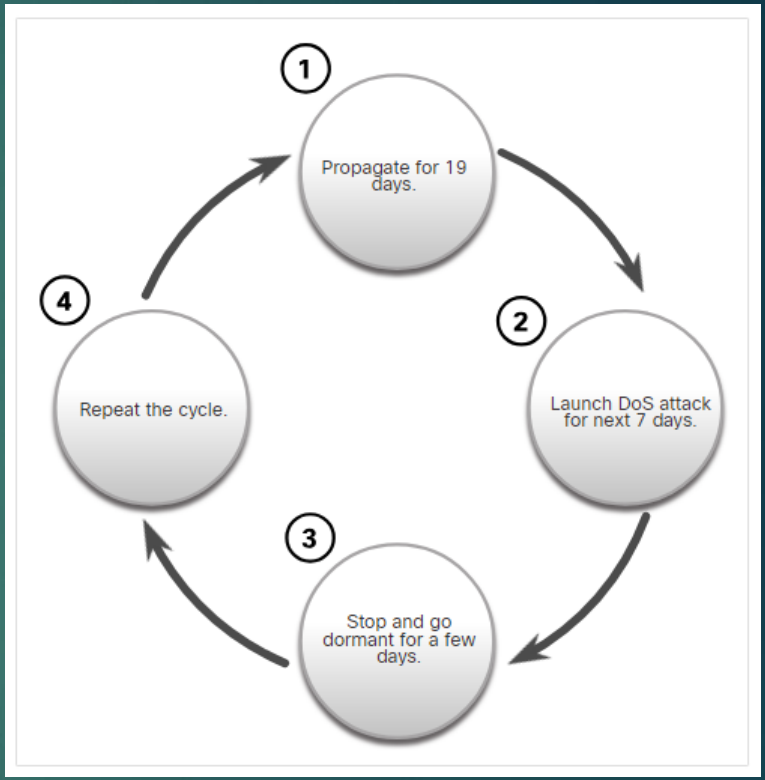


- The three worm components are as follows:
  - Enabling vulnerability - A worm installs itself using an exploit mechanism, such as an email attachment, an executable file, or a Trojan horse, on a vulnerable system.
  - Propagation mechanism - After gaining access to a device, the worm replicates itself and locates new targets.
  - Payload - Any malicious code that results in some action is a payload. Most often this is used to create a backdoor that allows a threat actor to access the infected host or to create a DoS attack.

Common Threats and Attacks

Worm Components (Contd.)

- Worms are self-contained programs that attack a system to exploit a known vulnerability.
- Upon successful exploitation, the worm copies itself from the attacking host to the newly exploited system and the cycle begins again.
- This propagation mechanism is commonly deployed in a way that is difficult to detect.
- **Note**: Worms never stop spreading on the internet. After they are released, worms continue to propagate until all possible sources of infection are properly patched.



Code Red Worm Propagation

Common Threats and Attacks

Ransomware

- Ransomware is a malware that denies access to the infected computer system or its data.
- Ransomware frequently uses an encryption algorithm to encrypt system files and data.
- Email and malicious advertising, also known as malvertising, are vectors for ransomware campaigns.
- Social engineering is also used, when cybercriminals pretending to be security technicians make random calls at homes and persuade users to connect to a website that downloads ransomware to the user's computer.

Common Threats and Attacks

Common Malware Behaviors

- Computers infected with malware often exhibit one or more of the following symptoms:
  - Appearance of strange files, programs, or desktop icons
  - Antivirus and firewall programs are turning off or reconfiguring settings
  - Computer screen is freezing or system is crashing
  - Emails are spontaneously being sent without your knowledge to your contact list
  - Files have been modified or deleted
  - Increased CPU and/or memory usage
  - Problems connecting to networks
  - Slow computer or web browser speeds
  - Unknown processes or services running
  - Unknown TCP or UDP ports open
  - Connections are made to hosts on the Internet without user action
  - Strange computer behavior
- **Note:** Malware behavior is not limited to the above list.

Types of Malware (Cont.)

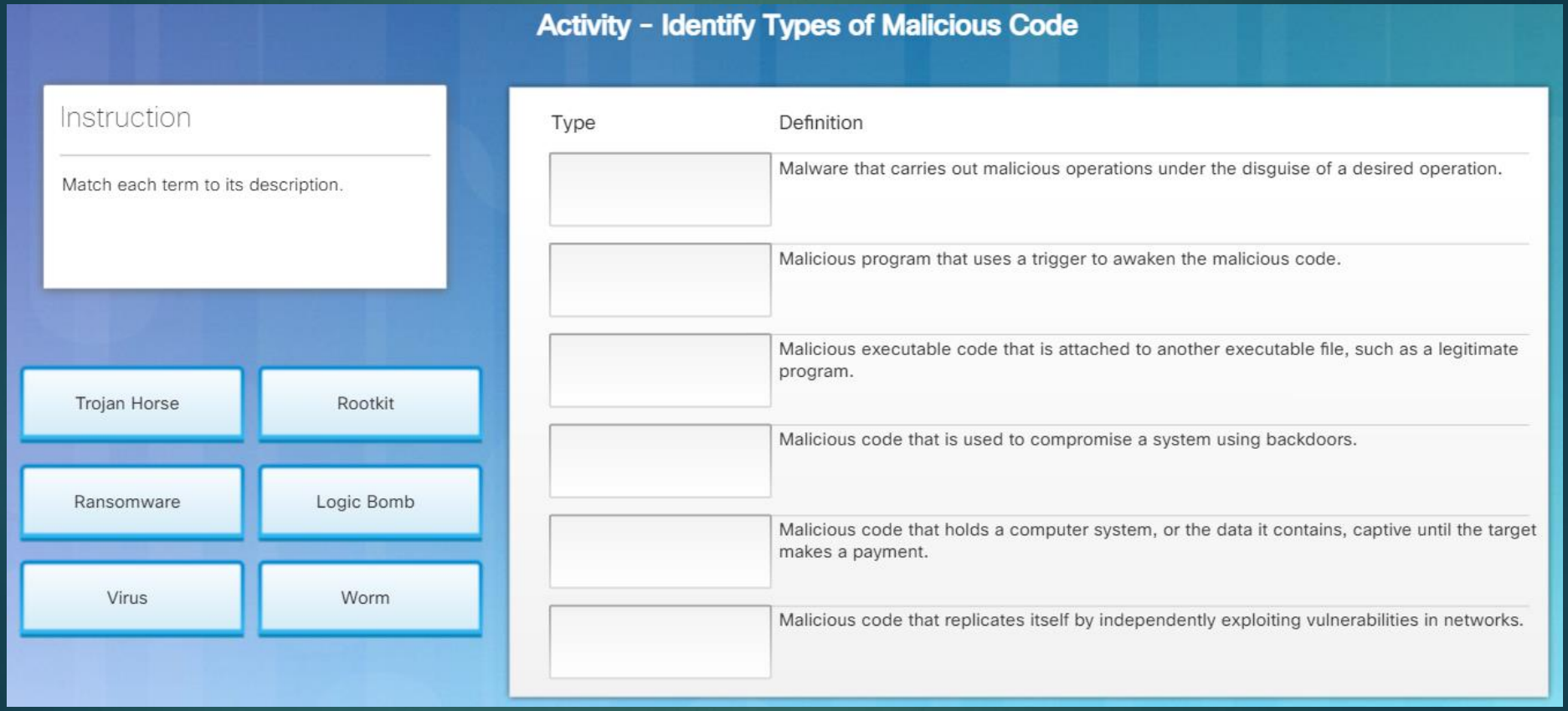
A few simple steps can help defend against all forms of malware:

- **Antivirus Program -** The majority of antivirus suites catch most widespread forms of malware.
- **Up-to-Date Software -** Many forms of malware achieve their objectives through exploitation of vulnerabilities in software, both in the operating system and applications.

5 of the Worst Computer Viruses Ever

Cybersecurity Threats, Vulnerabilities, and Attacks

Malware



Email and Browser Attacks

- **Spam -** also known as junk mail, is unsolicited email.
  - Watch for some of the more common indicators of spam:
  - An email has no subject line.
  - An email is requesting an update to an account.
  - The email text has misspelled words or strange punctuation.
  - Links within the email are long and/or cryptic.
  - An email looks like correspondence from a legitimate business.
  - The email requests that the user open an attachment.
- **Spyware** - track and spy on the user
- **Adware** - deliver advertisements, usually comes with spyware.
- **Scareware** - persuade the user to take a specific action based on fear.

Email and Browser Attacks

- **Phishing --** malicious party sends a fraudulent email disguised as being from a legitimate, trusted source, trick the recipient into installing malware on their device or sharing personal or financial information
- **Spear phishing --** a highly targeted phishing attack, emails are customized to a specific person.
- **Vishing --** is phishing using voice communication technology
- **Smishing --** (Short Message Service phishing) is phishing using text messaging on mobile phones.
- **Pharming --** is the impersonation of a legitimate website in an effort to deceive users into entering their credentials.
- **Whaling --** is a phishing attack that targets high profile targets within an organization such as senior executives. These could include politicians or celebrities.

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 - 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.

Email and Browser Attacks

- Defending Against Email and Browser Attacks
  - Filtering email
  - Educating the user
  - Keeping all software updated ensures that the system has all of the latest security patches

Cybersecurity Threats, Vulnerabilities, and Attacks

Email and Browser Attacks

Deception

The Art of Deception

Social Engineering - Social engineering is an attack that attempts to manipulate individuals into performing actions or divulging confidential information.

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.

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.

Types of Deception

Social engineers rely on several tactics. Social engineering tactics include:

Defending Against Deception

Organizations need to promote awareness of social engineering tactics and properly educate employees on prevention measures, such as the following:

- Never provide confidential information or credentials via email, chat sessions, in-person, or on the phone to unknown parties.
- Resist the urge to click on enticing emails and website links.
- Keep an eye out for uninitiated or automatic downloads.
- Establish policies and educate employees about those policies.
- When it comes to security, give employees a sense of ownership.
- Do not fall to pressure from unknown individuals.

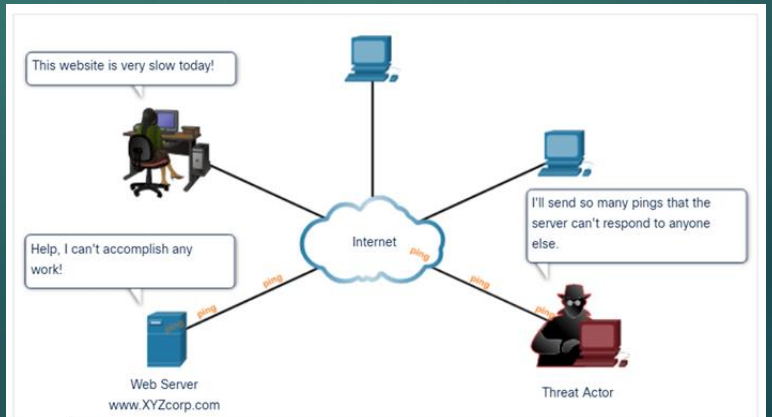
Attacks

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.

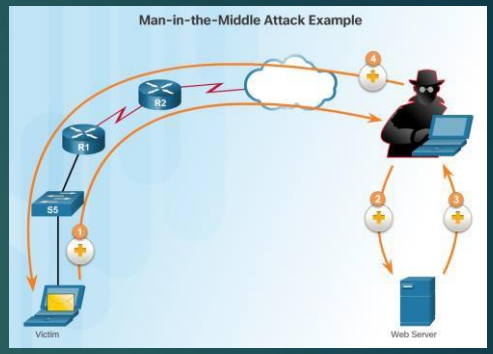
Spoofing - Spoofing is an impersonation attack, and it takes advantage of a trusted relationship between two systems. If two systems accept the authentication accomplished by each other, an individual logged onto one system might not go through an authentication process again to access the other system.



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.

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.

Defending Against Attacks

Configure firewalls to discard any packets from outside of the network that have addresses indicating that they originated from inside the network.

To prevent DoS and DDoS attacks, ensure patches and upgrades are current, distribute the workload across server systems.

Block external Internet Control Message Protocol (ICMP) packets at the border.

Encrypting traffic, providing cryptographic authentication, and including a time stamp with each portion of the message.

Wireless and Mobile Attacks (Cont.)

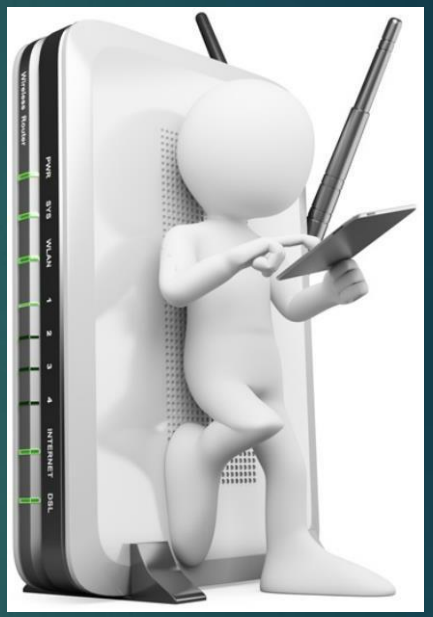
Grayware and SMiShing

- 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.

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.

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.

Ted Talk – All your devices can be hacked

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) - XSS allows criminals to inject scripts into the web pages viewed by users. . Cross-site scripting has three participants: the criminal, the victim, and the website.

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.

Application Attacks

Remote Code Executions 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.

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.

Module Summary

Summary

This module explained the structure of the cybersecurity world and the reason it continues to grow with data and information as the prized currency.

It explored the motivation of cyber criminals.

It explored the spread of threats due to the ever-expanding technical transformations taking place throughout the world.

It provided details on how to become a cybersecurity specialist to help defeat the cyber criminals.

It surveyed the resources available to help create more cybersecurity experts.

It discussed the various cybersecurity attacks that cyber criminals launch.

It explained the threat of malware and malicious code.

It discussed the types of deception involved with social engineering.

It explained the types of attacks that both wired and wireless networks experience.

Finally, it discussed the vulnerabilities presented by application