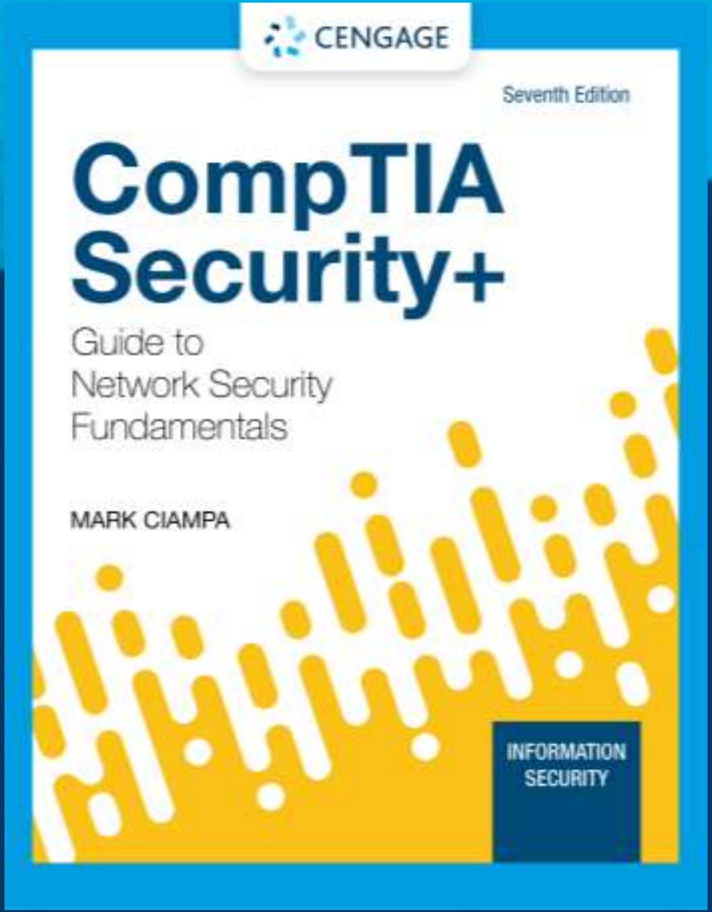


CompTIA Security+ Guide to Network Security Fundamentals, 7th Edition

Module 3: Threats and Attacks on Endpoints

CENGAGE

Module Objectives

By the end of this module, you should be able to:

1. Identify the different types of attacks using malware

2. Define application attacks

3. Explain how threat actors use application attacks

4. Define adversarial artificial intelligence attacks

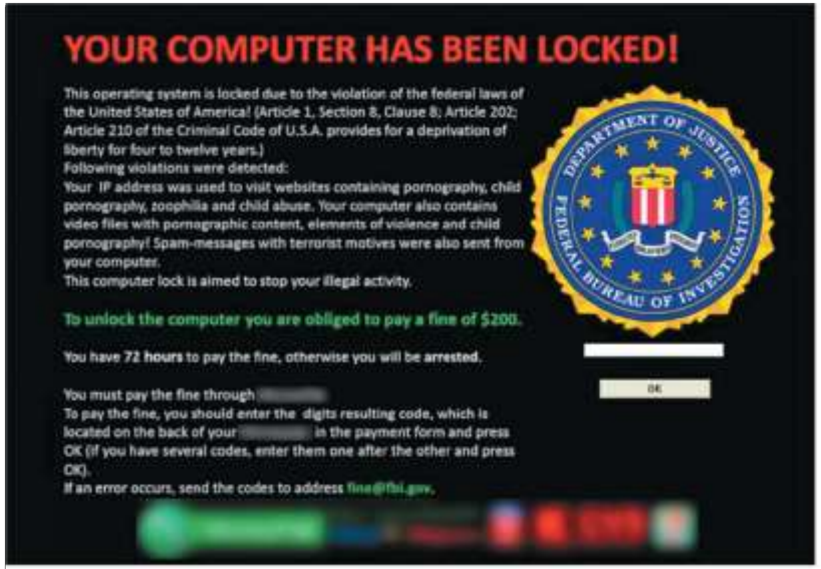
Attacks Using Malware

- **Malware** is software that enters a computer system without the user’s knowledge or consent and then performs an unwanted and harmful action
    - Malware is most often used as the general term that refers to a wide variety of damaging software programs
- Malware is continually evolving to avoid detection by improved security measures
- One attempt at classifying the diverse types of malware can be to examine the primary action that the malware performs:
    - Imprison
    - Launch
    - Snoop
    - Deceive
    - Evade

Imprison (1 of 4)

- Some types of malware attempt to take away the freedom of the user to do what they want
- Types of malware that imprisons are ransomware and cryptomalware
- Ransomware
  - **Ransomware** prevents a user’s endpoint device from properly and fully functioning until a fee is paid
  - Some ransomware pretends to come from a law enforcement agency while others pretend to come from a software vendor and displays a fictitious warning that a license has expired

Imprison (2 of 4)



YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)
Following violations were detected:
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.
This computer lock is aimed to stop your illegal activity.

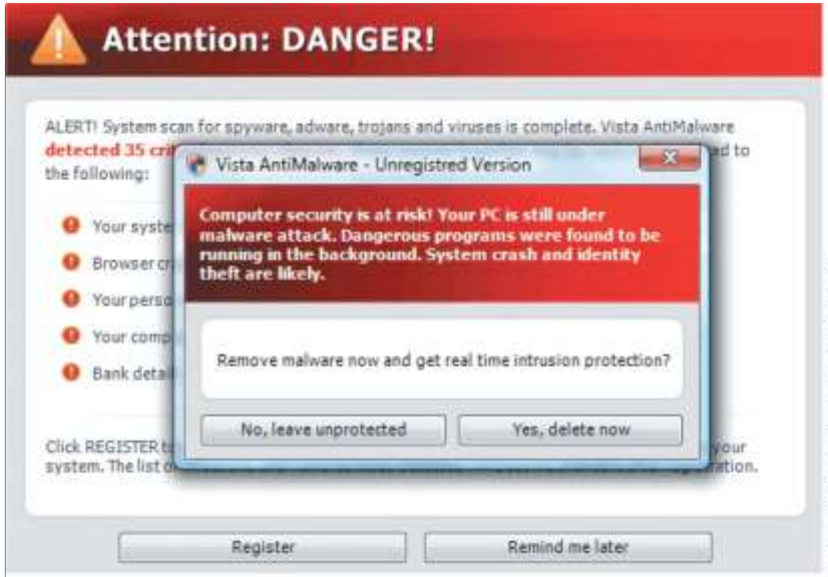
To unlock the computer you are obliged to pay a fine of $200.

You have **72 hours** to pay the fine, otherwise you will be **arrested.**

You must pay the fine through [redacted]
To pay the fine, you should enter the digits resulting code, which is located on the back of your [redacted] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).
If an error occurs, send the codes to address fine@fbi.gov.

Source: Symantec Security Response

Figure 3-1 Blocker ransomware message



Attention: DANGER!

ALERT! System scan for spyware, adware, trojans and viruses is complete. Vista AntiMalware **detected 35 cri** ...ed to the following:

- Your syste
- Browser cr
- Your perso
- Your comp
- Bank detai

Click REGISTER t... your system. The list o... ation.

Vista AntiMalware - Unregistred Version

Computer security is at risk! Your PC is still under malware attack. Dangerous programs were found to be running in the background. System crash and identity theft are likely.

Remove malware now and get real time intrusion protection?

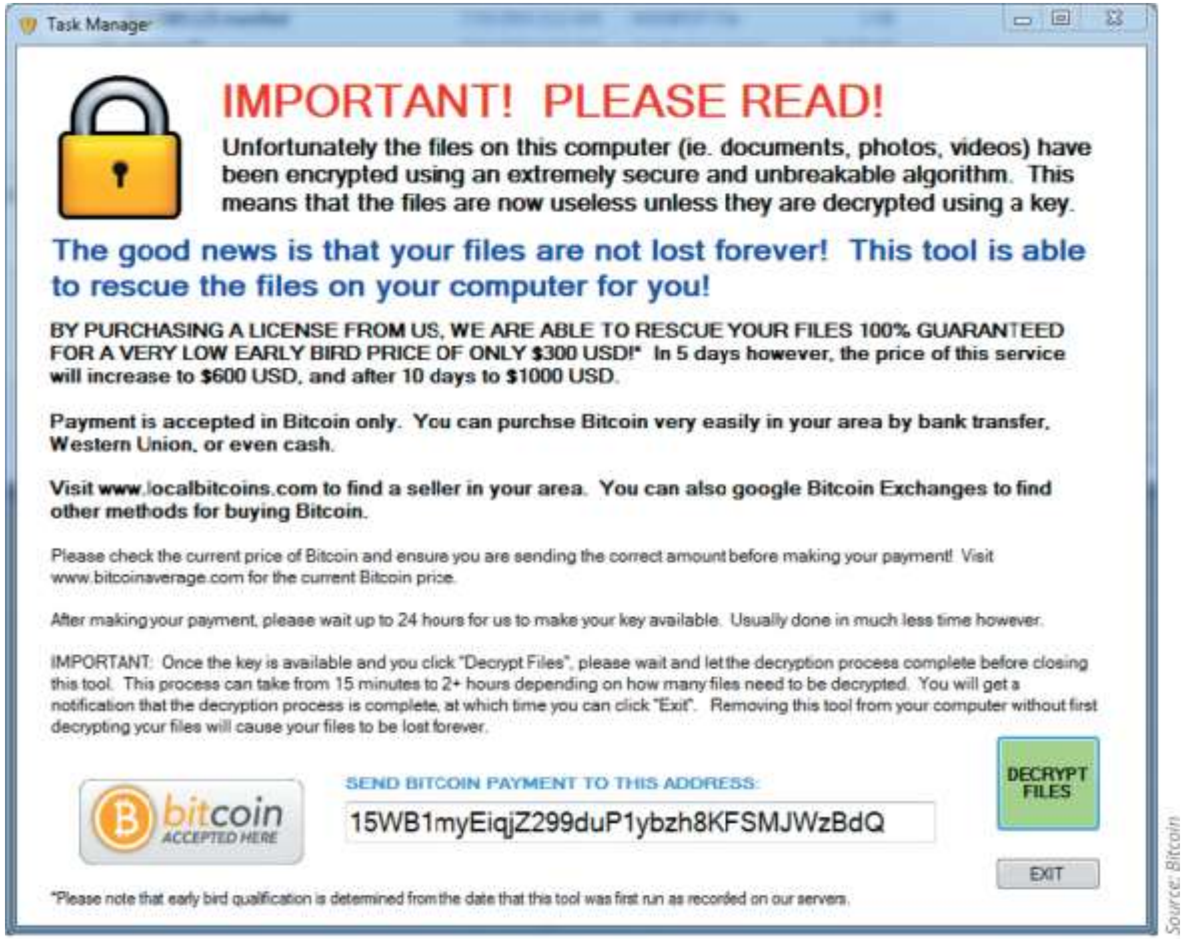
Source: Used with permissions from Microsoft

Figure 3-2 Ransomware computer infection

Imprison (3 of 4)

- Cryptomalware
  - **Cryptomalware** is a type of malware that imprisons users and encrypts all files on the device so that none of them can be opened
  - The cost for the key to unlock the cryptomalware increases every few hours or days
  - New variants of cryptomalware encrypt all files on any network or attached device connected to that computer

Imprison (4 of 4)



IMPORTANT! PLEASE READ!

Unfortunately the files on this computer (ie. documents, photos, videos) have been encrypted using an extremely secure and unbreakable algorithm. This means that the files are now useless unless they are decrypted using a key.

The good news is that your files are not lost forever! This tool is able to rescue the files on your computer for you!

BY PURCHASING A LICENSE FROM US, WE ARE ABLE TO RESCUE YOUR FILES 100% GUARANTEED FOR A VERY LOW EARLY BIRD PRICE OF ONLY $300 USD!* In 5 days however, the price of this service will increase to $600 USD, and after 10 days to $1000 USD.

Payment is accepted in Bitcoin only. You can purchse Bitcoin very easily in your area by bank transfer, Western Union, or even cash.

Visit www.localbitcoins.com to find a seller in your area. You can also google Bitcoin Exchanges to find other methods for buying Bitcoin.

Please check the current price of Bitcoin and ensure you are sending the correct amount before making your payment! Visit www.bitcoinaverage.com for the current Bitcoin price.

After making your payment, please wait up to 24 hours for us to make your key available. Usually done in much less time however.

IMPORTANT: Once the key is available and you click "Decrypt Files", please wait and let the decryption process complete before closing this tool. This process can take from 15 minutes to 2+ hours depending on how many files need to be decrypted. You will get a notification that the decryption process is complete, at which time you can click "Exit". Removing this tool from your computer without first decrypting your files will cause your files to be lost forever.

SEND BITCOIN PAYMENT TO THIS ADDRESS:

15WB1myEiqjZ299duP1ybzh8KFSMJWzBdQ

*Please note that early bird qualification is determined from the date that this tool was first run as recorded on our servers.

Source: Bitcoin

Figure 3-3 Cryptomalware message

Figure 3-3 Cryptomalware message

Launch (1 of 5)

- Malware that infects a computer to launch attacks on other computers includes a virus, worm, and bot
- Virus
  - There are two types of viruses: a file-based virus and a fileless virus
  - A *file-based virus* is malicious code that is attached to a file that reproduces itself on the same computer without any human intervention
  - An *armored file-based virus* goes to great lengths to avoid detection
    - Techniques include *split infection* and *mutation*
  - The virus first unloads a payload to perform a malicious action, then the virus replicates itself by inserting its code into another file (on the same computer)

Launch (2 of 5)

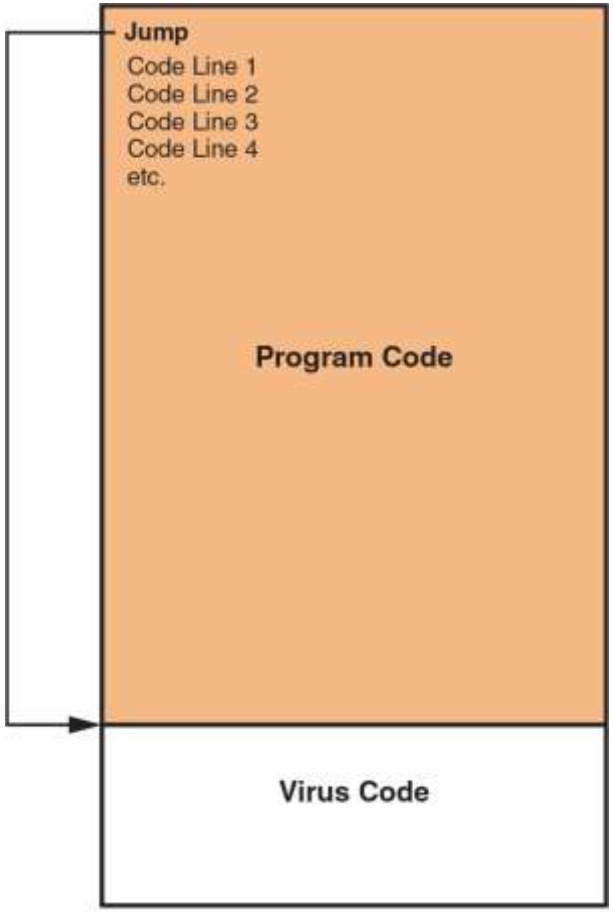


Figure 3-4 Appender infection

Figure 3-4 Appender infection

Launch (3 of 5)

- A **fileless virus** does not attach itself to a file but instead takes advantage of native services and processes that are part of the OS to avoid detection and carry out its attacks
  - It does not infect a file, instead the code is loaded directly in the computer’s random access memory (RAM)
- Advantages of a fileless virus over a file-based virus:
  - *Easy to infect*
  - *Extensive control*
  - *Persistent*
  - *Difficult to detect*
  - *Difficult to defend against*

Launch (4 of 5)

- Worm
  - A **worm** is a malicious program that uses a computer network to replicate (sometimes called a network virus)
  - Designed to enter a computer through the network and then take advantage of a vulnerability in an application or an OS on the host computer
  - Today’s worms can leave behind a payload on the systems they infect and cause harm, much like a virus
  - Actions that worms have performed include deleting files on the computer or allowing the computer to be remotely controlled by an attacker

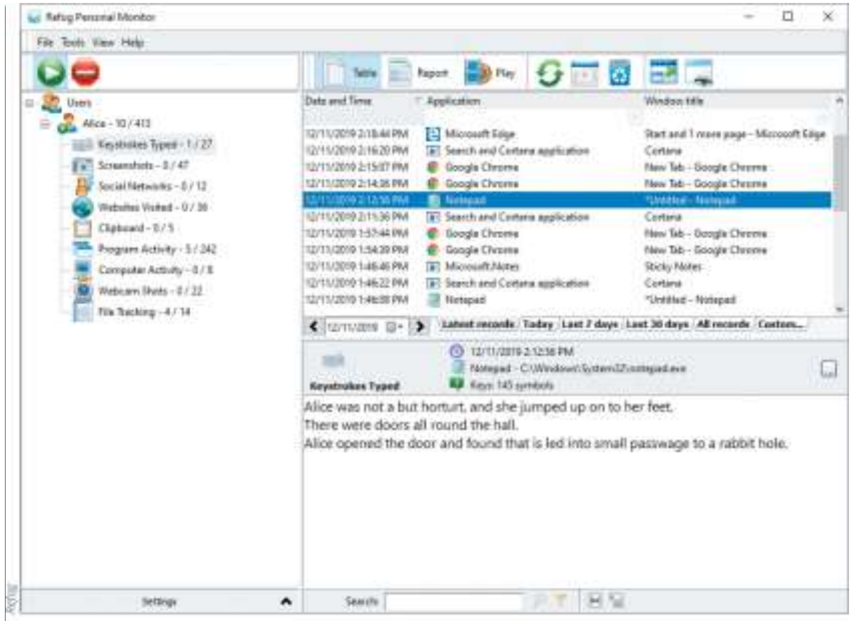
Launch (5 of 5)

- Bot
  - Another type of malware allows the infected computer to be placed under the remote control of an attacker for the purpose of launching attacks
  - The infected robot computer is known as a **bot** or *zombie*
  - When hundreds, thousands, or even millions of bot computers are gathered into a logical computer network, they create a *botnet* under the control of a *bot herder*
  - Infected bot computers receive instructions through a command and control (C&C) structure from the bot herders

Snoop (1 of 2)

- Two common types of snooping malware are spyware and keyloggers
- Spyware
  - **Spyware** is tracking software that is deployed without the consent or control of the user
- Keylogger
  - A **keylogger** silently captures and stores each keystroke that a user types on the computer’s keyboard
  - The threat actor can then search the captured text for any useful information such as passwords, credit card numbers, or personal information
  - A keylogger can be a software program or a small hardware device

Snoop (2 of 2)



Date and Time	Application	Window title
12/11/2019 2:18:44 PM	Microsoft Edge	Start and 1 more page – Microsoft Edge
12/11/2019 2:16:20 PM	Search and Cortana application	Cortana
12/11/2019 2:15:07 PM	Google Chrome	New Tab – Google Chrome
12/11/2019 2:14:36 PM	Google Chrome	New Tab – Google Chrome
12/11/2019 2:12:56 PM	Notepad	*Untitled – Notepad
12/11/2019 2:11:36 PM	Search and Cortana application	Cortana
12/11/2019 1:57:44 PM	Google Chrome	New Tab – Google Chrome
12/11/2019 1:54:39 PM	Google Chrome	New Tab – Google Chrome
12/11/2019 1:46:46 PM	Microsoft.Notes	Sticky Notes
12/11/2019 1:46:22 PM	Search and Cortana application	Cortana
12/11/2019 1:46:08 PM	Notepad	*Untitled – Notepad

Keystrokes Typed

12/11/2019 2:12:38 PM
Notepad - C:\Windows\System32\notepad.exe
Keys: 145 symbols

Alice was not a but horturt, and she jumped up on to her feet.
There were doors all round the hall.
Alice opened the door and found that is led into small passwage to a rabbit hole.

Figure 3-5 Software keylogger

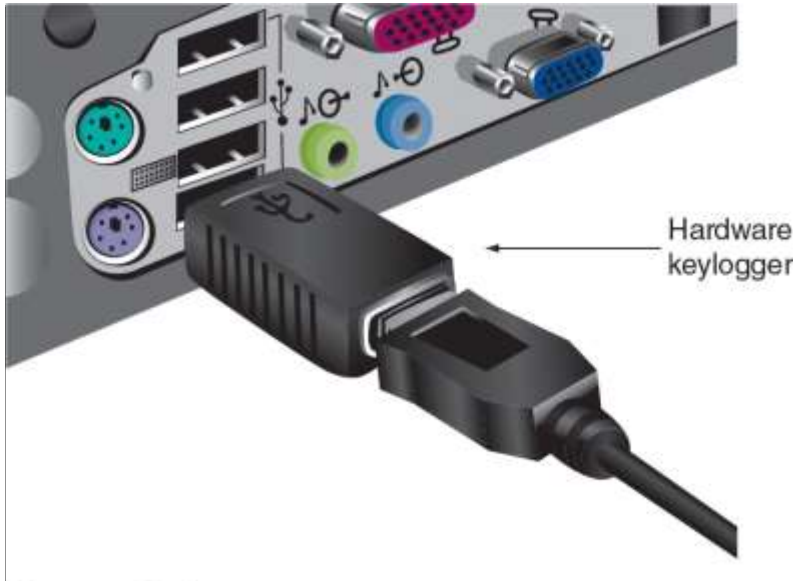


Figure 3-6 Hardware keylogger

Deceive (1 of 2)

- Some malware attempts to deceive the user and hide its true intentions
- Examples include potentially unwanted programs (PUPs), Trojans, and remote access Trojans (RATs)
- **Potentially Unwanted Program (PUP)**
  - A PUP is software that the user does not want on their computer
  - Examples of PUPs:
    - Advertising that obstructs content or interferes with web browsing, pop-up windows, pop-under windows, search engine hijacking, home page hijacking, etc

Deceive (2 of 2)

- Trojan
  - A computer **Trojan** is an executable program that masquerades as performing a benign activity but also does something malicious
- Remote Access Trojan (RAT)
  - A **RAT** has the basic functionality of a Trojan but also gives the threat agent unauthorized remote access to the victim’s computer by using specially configured communication protocols
  - This creates an opening to the victim’s computer allowing the threat agent unrestricted access

Evade

- This category of malware attempts to help malware or attacks evade detection
  - Includes backdoor, logic bomb, and rootkit
- Backdoor
  - A **backdoor** gives access to a computer, program, or service that circumvents any normal security protections
- Logic bomb
  - A **logic bomb** is computer code that is typically added to a legitimate program but lies dormant and evades detection until a specific logical event triggers it
- Rootkits
  - A **rootkit** is malware that can hide its presence and the presence of other malware on the computer
    - It does this by accessing “lower layers” of the OS to make alterations

Knowledge Check Activity 1

What is the primary action that cryptomalware performs?

a. Imprison

b. Launch

c. Snoop

d. Deceive

Knowledge Check Activity 1: Answer

What is the primary action that cryptomalware performs?

Answer: a. Imprison

This type of malware imprisons users and encrypts all files on the device so that none of them can be opened without a key for which the victim must pay the attacker.

Application Attacks

- Another category of attacks look for vulnerabilities in applications or manipulate applications in order to compromise them
  - Common targets of attackers using application attacks are Internet web server
- A web server provides services that are implemented as “web applications” through software applications running on the server

Scripting

- In a **cross-site scripting** (**XSS**) attack, a website that accepts user input without validating it and uses that input in a response can be exploited
- An attacker can take advantage in an XSS attack by tricking a valid website into feeding a malicious script to another user’s web browser

Injection

- Attacks called **injections** introduce new input to exploit a vulnerability
- One of the most common injection attacks (**SQL injection**) inserts statements to manipulate a database server
- SQL stands for **Structured Query Language**
- SQL injection targets SQL servers by introducing malicious commands into them
- By entering crafted SQL statements as user input, information from the database can be extracted or the existing can be manipulated

Request Forgery (1 of 4)

- *Request forgery* is a request that has been fabricated
- There are two types of request forgeries:
  - **Cross-site request forgery (CSFR)** and a **server-site request forgery (SSRF)**
- Cross-Site Request Forgery (CSRF)
  - CSRF takes advantage of an authentication "token" that a website sends to a user's web browser
  - If a user is currently authenticated on a website and is then tricked into loading another webpage, the new page inherits the identity and privileges of the victim, who may the perform an undesired function on the attacker's behalf

Request Forgery (2 of 4)

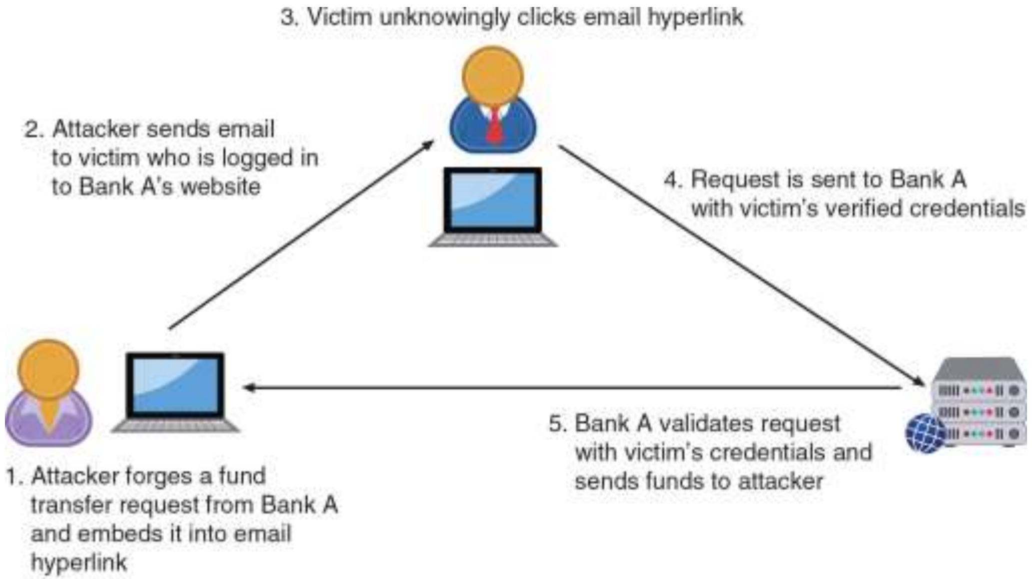

3. Victim unknowingly clicks email hyperlink
2. Attacker sends email to victim who is logged in to Bank A's website
4. Request is sent to Bank A with victim's verified credentials
5. Bank A validates request with victim's credentials and sends funds to attacker
1. Attacker forges a fund transfer request from Bank A and embeds it into email hyperlink

Figure 3-11 Cross-site request forgery

Figure 3-11 Cross-site request forgery

Request Forgery (3 of 4)

- Server-Site Request Forgery (SSRF)
  - An SSRF takes advantage of a trusting relationship between web servers
  - SSRF attacks exploit how a web server processes external information received from another server
  - Some web applications are designed to read information from or write information to a specific URL
  - If an attacker can modify that target URL, they can potentially extract sensitive information from the application or inject untrusted input into it

Request Forgery (4 of 4)

Attack Name	Attack Target	Purpose of Attack
CSRF	User	Force target to take action for attacker while pretending to be authorized user
SSRF	Web server	Gain access to sensitive data or inject harmful data

Replay

- Replay attacks are commonly used against digital identities
  - After intercepting and copying data, the threat actor retransmits selected and edited portions of the copied communications later to impersonate the legitimate user
- Many digital identity replay attacks are between a user and an authentication server

Attacks on Software (1 of 3)

- Other attacks are directly focused on vulnerabilities in the software applications
- These include:
  - Exploiting memory vulnerabilities
  - Improper exception and error handling
  - External software components
- Memory Vulnerabilities
  - Some memory-related attacks are called **resource exhaustion** attacks because they “deplete” parts of memory and thus interfere with the normal operation of the program in RAM
  - Other memory-related attacks attempt to manipulate memory contents such as buffer overflow attacks and integer overflow attacks

Attacks on Software (2 of 3)

- Memory Vulnerabilities (continued)
  - A **buffer overflow attack** occurs when a process attempts to store data in RAM beyond the boundaries of a fixed-length storage buffer
    - This extra data overflows into the adjacent memory locations
  - In an **integer overflow attack**, an attacker changes the value of a variable to something outside the range that the programmer had intended by using an integer overflow
- Improper Exception Handling
  - Some attacks are the result of poor coding on the part of software developers
  - Software that allows the user to enter data but has **improper input handling** features does not filter or validate user input to prevent a malicious action
  - Another improper exception handling situation is a NULL **pointer/object dereference**
    - When an application dereferences a pointer that has a value of NULL, it typically will cause a program to crash or exit

CENGAGE

Attacks on Software (3 of 3)

- Attacks on External Software Components
  - In addition to attacking the software directly, threat actors also target external software components
  - These include the following:
    - *Application program interface (API)*
    - *Device driver*
    - *Dynamic-link library (DLL)*

Knowledge Check Activity 2

Which type of application attack might use the following syntax?

‘*whatever*’ AND *email* IS NULL;

a. Cross-site scripting

b. Client-side request forgery

c. SQL injection

d. Buffer overflow

Knowledge Check Activity 2: Answer

Which type of application attack might use the following syntax?

‘*whatever*’ AND *email* IS NULL;

Answer: c. SQL injection

An SQL injection attack inserts statements to manipulate a database server. The statement in the question can determine the names of different fields in the database.

Adversarial Artificial Intelligence Attacks

- Cybersecurity is using artificial intelligence to enhance the detection of malicious behavior and advanced threats
  - However, there are significant vulnerabilities and risks with using these new tools
- Understanding them includes:
  - Knowing what the tools are and what they can do
  - How these tools are used in cybersecurity
  - Knowing their potential risks

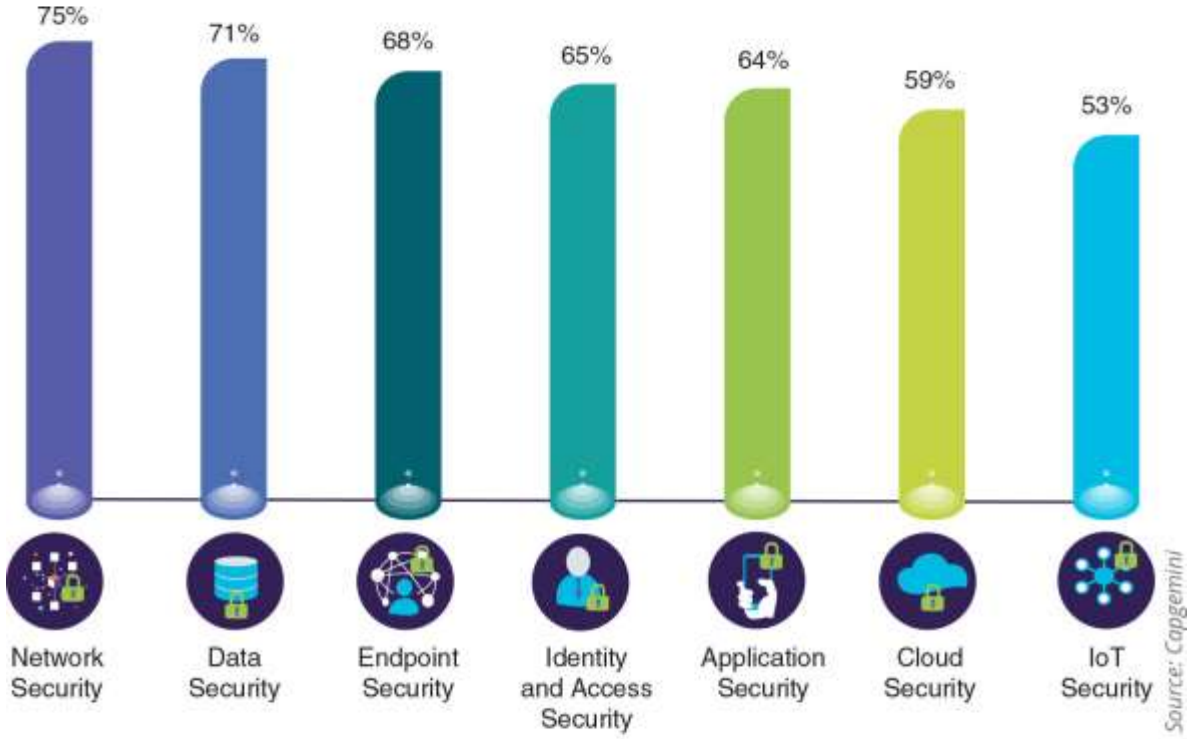
What Are Artificial Intelligence (AI) and Machine Learning (ML)?

- The definitions of AI vary, but *AI* may be defined as technology that imitates human abilities
- A recognized subset of AI is *machine learning* (*ML*)
    - ML is defined as “teaching” a technology device to “learn” by itself without the continual instructions of a computer programmer
- ML also involves learning through repeated experience
    - If something attempted does not work, then it determines how it could be changed to make it work

Uses in Cybersecurity (1 of 2)

- Cybersecurity AI allows organizations to detect, predict, and respond to cyberthreats in real time using ML
- Virtually all email systems use some type of AI to block phishing attacks
- The prime advantages of using AI to combat threats are continual learning and greater speed in response
  - AI can predict and prevent future attacks
- About one in five organizations used cybersecurity AI before 2019
  - Increasing to two out of three organizations planning to deploy it by the end of 2020

Uses in Cybersecurity (2 of 2)



Source: Capgemini

Figure 3-13 How AI cybersecurity is used

Figure 3-13 How AI cybersecurity is used

Risks in Using AI and ML in Cybersecurity

- Risks associated with using AI and ML are called **adversarial artificial intelligence**
- The first risk is the **security of ML algorithms**
  - These could be attacked and compromised, allowing threat actors to alter algorithms to ignore attacks
- Another risk is **tainted training data for machine learning**
  - Attackers can attempt to alter the training data that is used by ML in order to produce false negatives to cloak themselves

Knowledge Check Activity 3

Which of the following is a concern of using AI and ML in cybersecurity?

a. Buffer overflows

b. Improper input handling

c. Device driver manipulation

d. Tainted training data

Knowledge Check Activity 3: Answer

Which of the following is a concern of using AI and ML in cybersecurity?

Answer: d. Tainted training data

Attackers can attempt to alter training data that is used by machine learning in order to produce false negatives and cloak themselves.

Self-Assessment

1. Use the knowledge about malware you gained from this module to answer the following question: With the trend towards employees working from home, which type of malware do you think presents the most risk for organizations and their employees? Why? What are some things that can be done to mitigate the risks?

Summary (1 of 2)

- The word “endpoint” is commonly used when referring to network-connected hardware devices
- Malware is software that enters a computer system without the user’s knowledge or consent and then performs an unwanted and harmful action
- Some types of malware attempt to take away the freedom of users
- Another category of malware infects a computer to then launch attacks on other computers
- Another category of malware “snoops” or spies on its victims
- Some malware attempts to deceive the user and hide its true intentions
- Some malware attempts to evade detection
- Another category of attacks specifically targets software applications that are already installed and running on the device

Summary (2 of 2)

- A cross-site request forgery (CSRF) takes advantage of an authentication "token" that a website sends to a user's web browser
- Several attacks are directed at vulnerabilities associated with how a program uses RAM
- Software that allows the user to enter data but has improper input handling features does not filter or validate user input to prevent a malicious action
- In an application program interface (API) attack, a threat actor looks for vulnerabilities in the API, a link provided by an OS, web browser, or other platform that allows a developer access to resources at a high level
- Artificial intelligence (AI) is technology that imitates human abilities