BongoDemy
A new way of learning

Essential Hacking Terms

BongoDemy
1351 East Barandi Para, Jessore - 7400
Khulna, Bangladesh
Contact: +8801722-769661
Email: support@bongodemy.com
Web: www.bongodemy.com

White Hat: White hat typically refers to ethical hackers or computer security experts who use their skills to identify and fix security vulnerabilities and protect computer systems from unauthorized access.

For example, a white hat hacker might be hired by a company to test the security of their computer systems and identify any weaknesses or vulnerabilities that could be exploited by malicious actors. Once the vulnerabilities are identified, the white hat hacker would then work with the company to fix them and strengthen their security defenses.

Another example of a white hat could be an individual who reports a security vulnerability or breach to the appropriate authorities or company, without exploiting it for their own gain. By reporting the vulnerability, they can help prevent others from exploiting it for malicious purposes, ultimately helping to improve security for everyone.

Black hat: Black hat typically refers to hackers or computer criminals who use their skills to gain unauthorized access to computer systems or networks for personal gain or malicious purposes.

For example, a black hat hacker might use techniques such as phishing or malware to gain access to a company's computer system, steal sensitive data such as credit card numbers or intellectual property, and then sell or exploit that information for their own benefit. They may also use their skills to disrupt or damage computer systems, often for political or ideological reasons.

Another example of a black hat could be an individual who creates and distributes viruses or malware with the intent of causing harm to computer systems or stealing personal information. They may use these tactics to gain access to bank accounts, steal identities, or blackmail individuals or companies.
It's important to note that these actions are illegal and can have severe consequences for those who engage in them.

Grey hat: Grey hat typically refers to hackers or computer security experts who use their skills to identify and expose security vulnerabilities in computer systems, networks, or applications without malicious intent, but without necessarily having permission from the owner or operator of the system they are testing.

For example, a grey hat hacker might discover a vulnerability in a company's computer system, and then publicly disclose the issue in order to bring attention to the problem and encourage the company to fix it. While their intentions may be good, this approach could still be seen as unethical, as it can expose sensitive information or put systems at risk without proper authorization.

Another example of a grey hat could be an individual who performs security assessments or penetration testing on computer systems for companies or organizations, but without explicit permission or a formal agreement in place. While their intent may be to identify and address security weaknesses, their actions could still be considered unethical or even illegal.

It's important to note that grey hat hacking can be a controversial topic, as there is often a fine line between identifying security vulnerabilities in a responsible manner and engaging in unauthorized hacking or cybercrime.

Attack: An attack refers to any attempt to exploit a vulnerability or weakness in a computer system or network, with the intention of gaining unauthorized access, stealing sensitive information, or causing damage to the system or network.

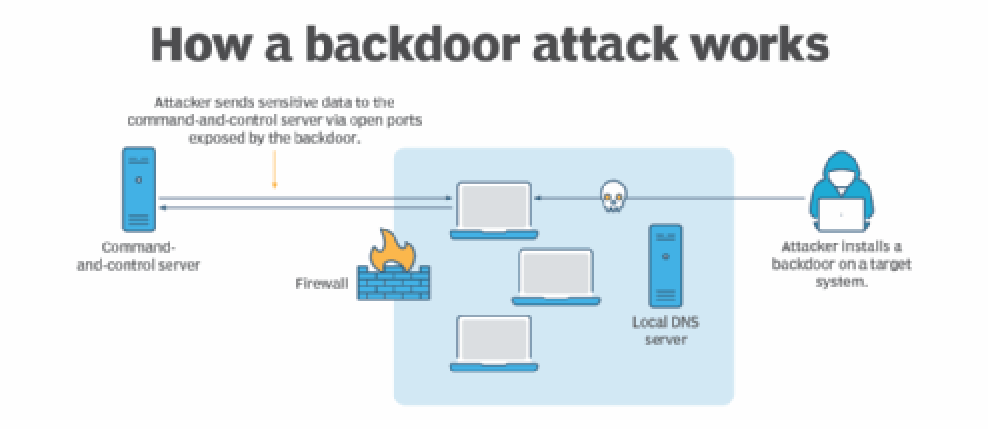
Here are a few examples of common types of attacks:

- Phishing: This is a type of attack where an attacker sends an email or message that appears to be from a trusted source, such as a bank or other reputable organization, in an attempt to trick the recipient into providing sensitive information such as passwords or credit card numbers.
- Malware: This is a type of software that is designed to harm or gain unauthorized access to a computer system. Examples of malware include viruses, worms, and Trojans, which can be spread through email attachments, downloads, or other means.
- Denial-of-Service (DoS) attack: This is a type of attack where an attacker floods a server or network with traffic or requests, with the intention of overwhelming the system and causing it to crash or become inaccessible to legitimate users.
- SQL Injection: This is a type of attack where an attacker inserts malicious code into a SQL database, with the intention of stealing or manipulating sensitive data.

- Man-in-the-Middle (MITM) attack: This is a type of attack where an attacker intercepts communications between two parties in order to eavesdrop or steal information.

It's important to note that these examples are just a few of the many types of attacks that can occur in the digital world. Defending against attacks requires a multi-layered approach that includes technical controls, user education, and best practices for security and privacy.

Back door: In the context of computer security, a backdoor is a hidden or undocumented method of bypassing normal authentication or access controls in a computer system or application. Backdoors can be created intentionally by developers or hackers, and can be used to gain unauthorized access to a system or to remotely control it without the knowledge or consent of the system owner or user.

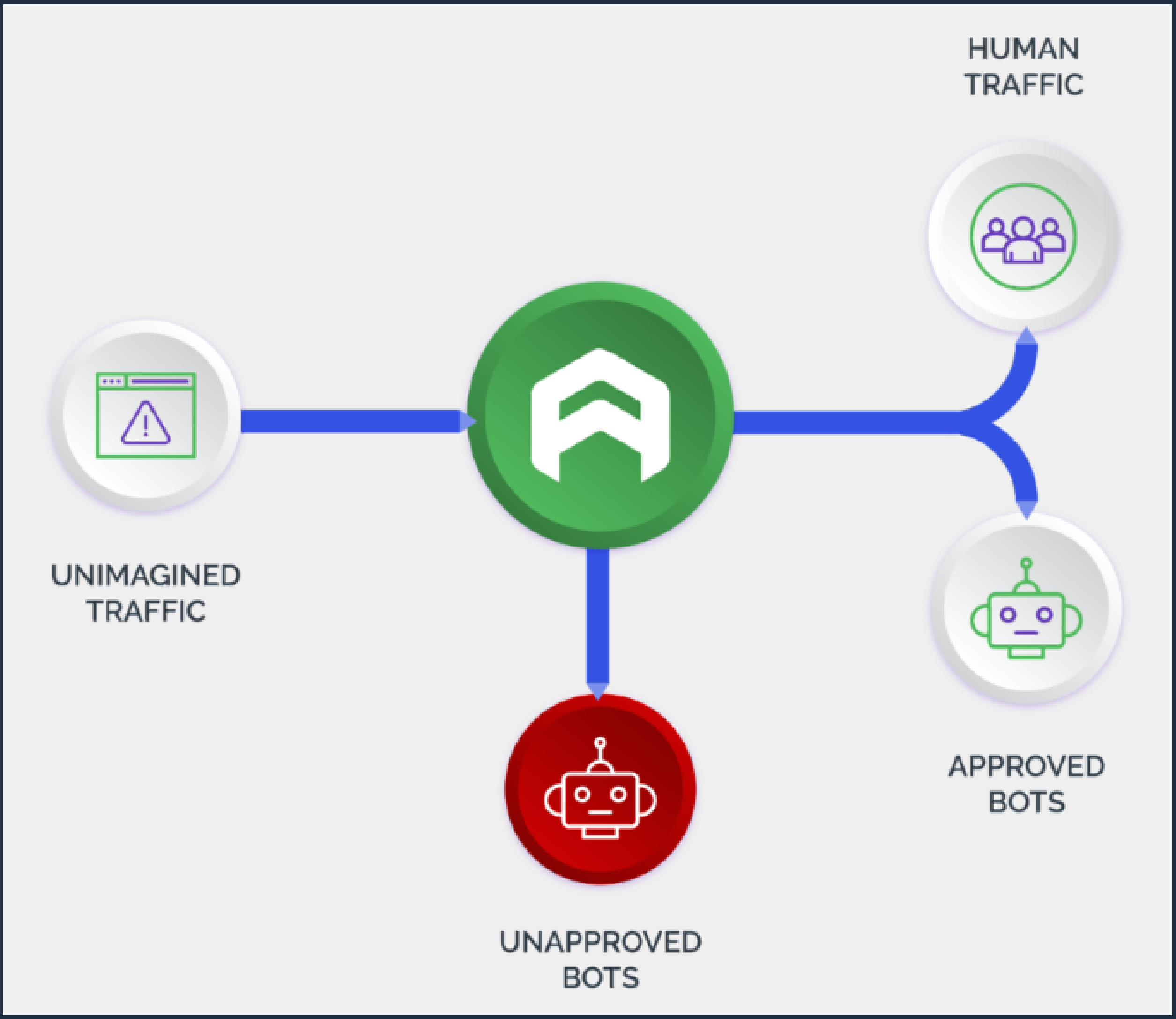

How a backdoor attack works
Attacker sends sensitive data to the command-and-control server via open ports exposed by the backdoor.
Command-and-control server
Firewall
Local DNS server
Attacker installs a backdoor on a target system.

Here's an example of how a backdoor might be used:
Imagine a company's network administrator installs a backdoor in the company's system that allows them to bypass normal authentication procedures and gain full access to the system. This backdoor could be used by the administrator to remotely control the system or steal sensitive information without being detected. This could have serious consequences for the company, including financial loss, damage to its reputation, and legal action.

In some cases, backdoors can be created inadvertently, such as when a developer forgets to remove debugging code or intentionally leaves a hardcoded password in a program. These types of backdoors can be just as dangerous as intentional ones, as they can also be exploited by malicious actors to gain unauthorized access to a system.

Detecting and closing backdoors is an important part of maintaining the security and integrity of computer systems and applications. This can be done through regular security audits, code reviews, and vulnerability assessments.

Bot: In the context of computing, a bot (short for "robot") refers to a type of software application that automates tasks that would otherwise be performed by a human. Bots can be programmed to perform a wide range of tasks, from simple tasks like web crawling and data collection to more complex tasks like natural language processing and machine learning.

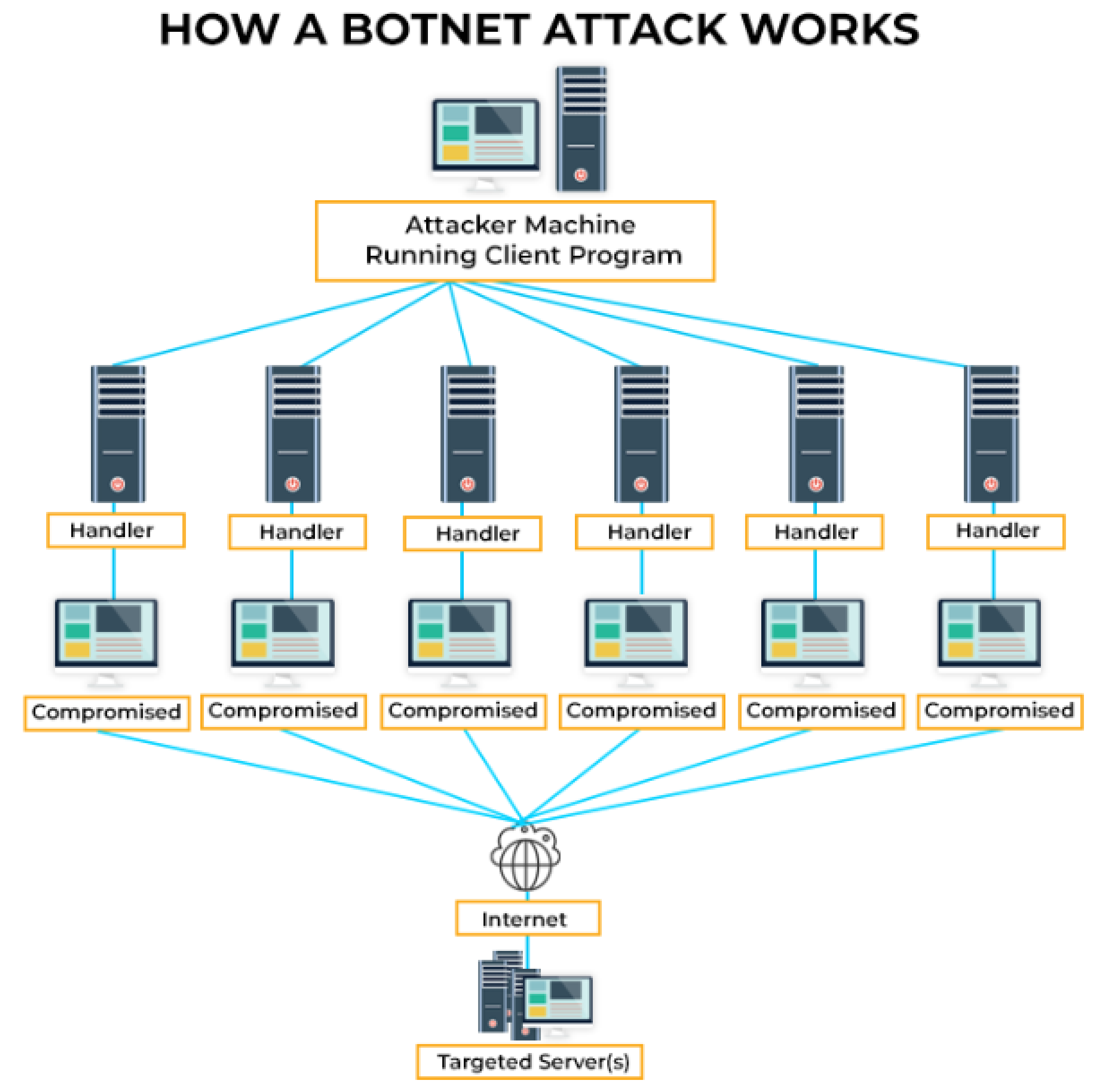


Here are a few examples of bots:

- Web crawlers: These bots are used by search engines like Google to automatically scan the internet and index web pages for search results.
- Chatbots: These bots are programmed to simulate human conversation and can be used for customer service, sales, or other types of interactions.
- Social media bots: These bots are used to automate social media activities such as liking, sharing, and commenting on posts. They can also be used to spread propaganda or misinformation.
- Trading bots: These bots are used in financial markets to automate trading activities, such as buying and selling stocks or cryptocurrencies.
- Game bots: These bots are used in online gaming to automate tasks such as farming resources or leveling up characters.

While bots can be useful in many contexts, they can also be used for malicious purposes, such as conducting cyber attacks or spreading spam or malware. As such, it's important to be aware of the potential risks associated with bots and to take steps to protect against them, such as implementing strong authentication and access controls, monitoring network traffic for suspicious activity, and using anti-malware software.

Botnet: A botnet is a network of computers that have been infected with malicious software, or "bots," that can be controlled remotely by an attacker. The attacker can use the botnet to carry out a range of nefarious activities, such as launching DDoS attacks, stealing sensitive information, or spreading malware.



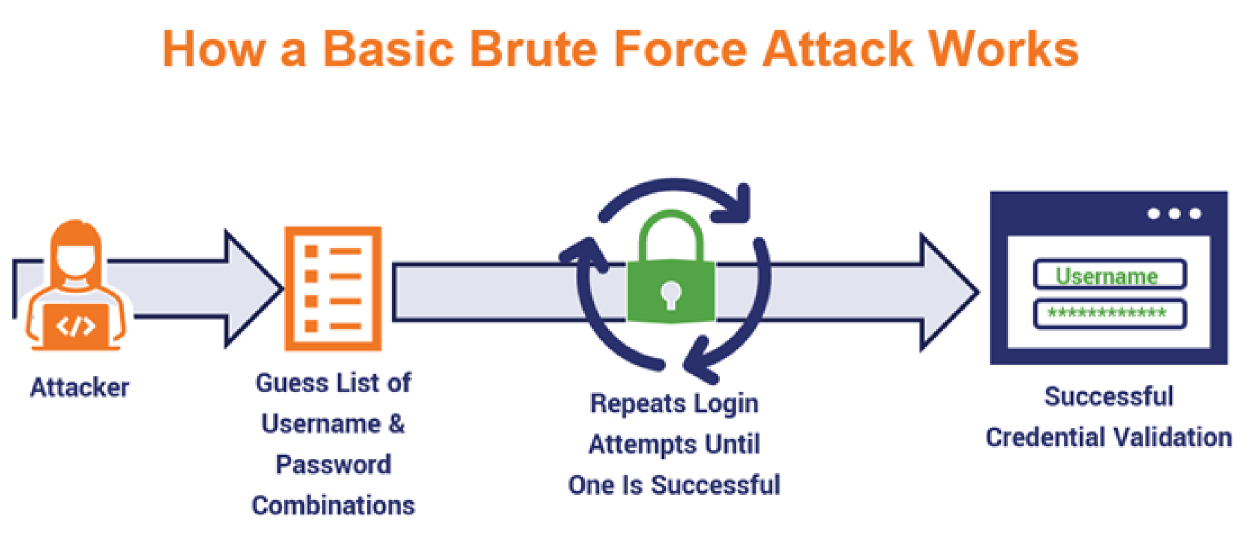
Here's an example of how a botnet might work:
Imagine an attacker creates a piece of malware that can infect a computer when a user clicks on a malicious link or downloads a file. Once the malware is installed on the computer, it can communicate with the attacker's command-and-control (C&C) server, which is used to issue commands to the infected computer.

The attacker can then use the botnet to carry out a variety of malicious activities, such as:

- DDoS attacks: The attacker can use the botnet to flood a website or server with traffic, overwhelming it and causing it to become unavailable to legitimate users.
- Spamming: The attacker can use the botnet to send out spam emails or messages, either for financial gain or to spread malware.
- Stealing data: The attacker can use the botnet to steal sensitive information from the infected computers, such as login credentials, financial data, or personal information.
- Cryptocurrency mining: The attacker can use the botnet to mine cryptocurrency, using the processing power of the infected computers to generate new coins.

Botnets can be difficult to detect and defend against, as they often involve large numbers of infected computers that are spread across multiple networks and locations. However, there are steps that can be taken to mitigate the risk of botnet attacks, such as keeping software up to date, using anti-malware software, and implementing strong security controls and access policies.

Brute force attack: A brute force attack is a type of cyberattack in which an attacker tries to gain unauthorized access to a system or application by repeatedly guessing passwords or encryption keys until they find the correct one. Brute force attacks are typically automated, using software that can generate and test a large number of password combinations in a short amount of time.


How a Basic Brute Force Attack Works
</>
Attacker
Guess List of Username & Password Combinations
Repeats Login Attempts Until One Is Successful
Username
****
Successful Credential Validation

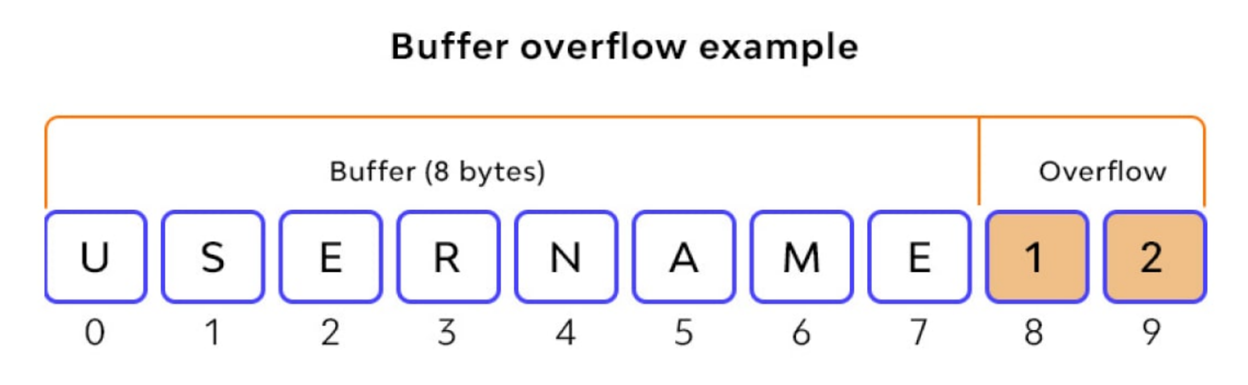
Here's an example of how a brute force attack might work:
Imagine an attacker wants to gain access to a user's online account on a website. The attacker begins by using a software program that generates a list of possible passwords, such as "password1," "password2," "password3," and so on. The attacker then uses another program that automatically tries each password on the website's login page, checking to see if any of them work.

If the attacker is lucky, they may guess the correct password on the first try. However, if the password is complex enough, it may take the attacker many thousands or even millions of attempts to find the correct one.

Brute force attacks can be used to target a wide range of systems and applications, from online accounts and email servers to encryption algorithms and other types of security measures. They are often used by hackers and other malicious actors to gain unauthorized access to sensitive data or to take control of systems for malicious purposes.

To protect against brute force attacks, it's important to use strong passwords and encryption keys that are difficult to guess, as well as implementing security controls and access policies that limit the number of login attempts allowed before a user is locked out. Additionally, implementing two-factor authentication or multi-factor authentication can also provide an extra layer of protection against brute force attacks.

Buffer overflow: A buffer overflow is a type of software vulnerability that occurs when a program tries to store more data in a buffer, or temporary storage area, than it can handle. This can cause the program to overwrite adjacent memory locations, which can lead to crashes, errors, or even allow an attacker to execute malicious code on the affected system.



Here's an example of how a buffer overflow might work:
Imagine a web application that has a login form that asks for a username and password. When a user enters their credentials, the application stores them in a buffer, which is a temporary storage area in the computer's memory.

However, if an attacker is able to enter a username or password that is longer than the buffer can handle, the program may try to store the extra data in adjacent memory locations, overwriting important data or even executing malicious code. For example, an attacker could enter a username that is much longer than the buffer can handle, causing the program to overwrite adjacent memory locations and execute a piece of code that gives the attacker remote access to the affected system.

Buffer overflows can be difficult to detect and prevent, as they often involve complex interactions between software components and memory management systems. However, there are steps that can be taken to reduce the risk of buffer overflow attacks, such as using secure coding practices, validating input data, and implementing software security controls and access policies that limit the amount of memory that can be accessed by a program or user.

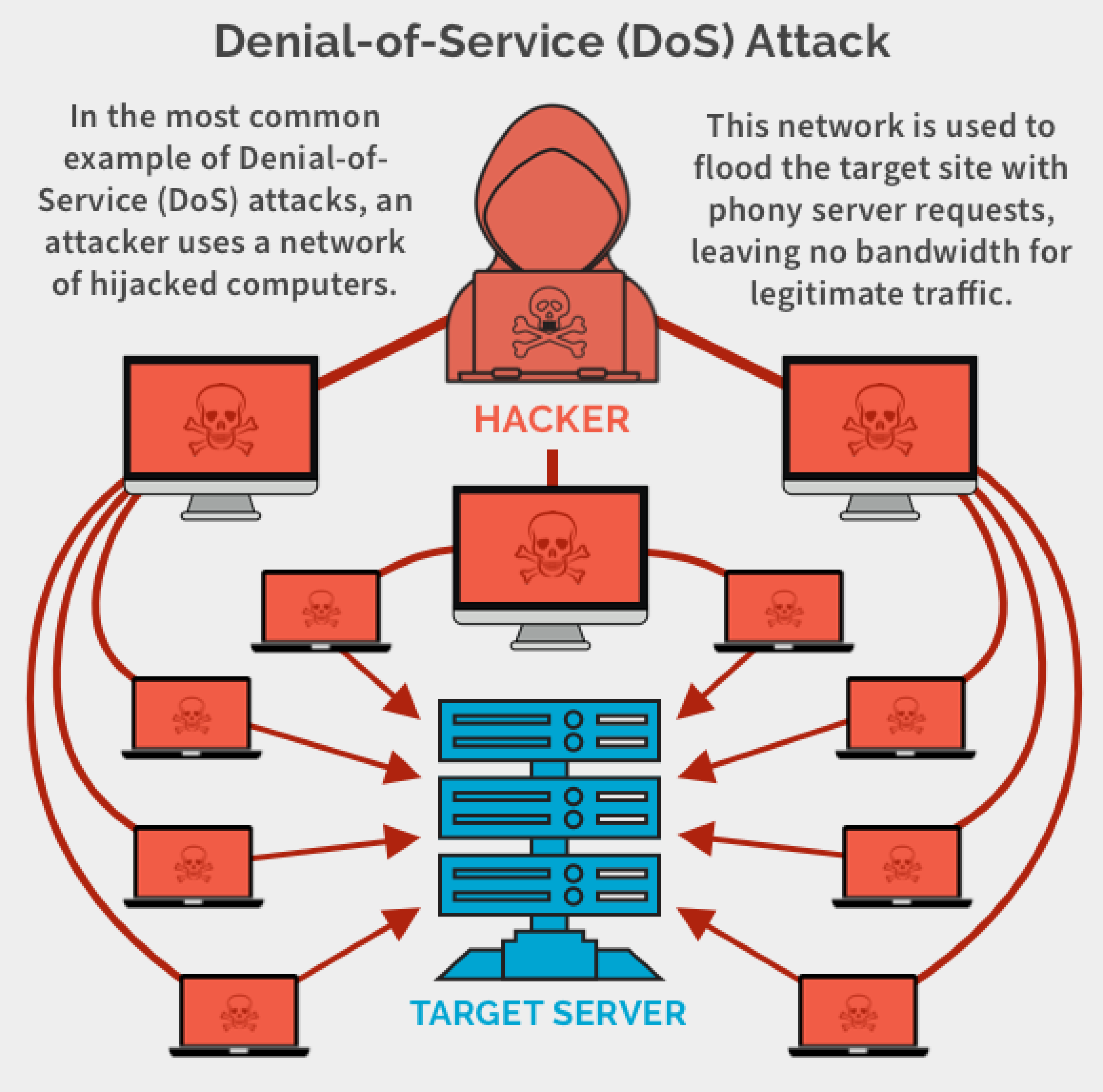
Cracker: A cracker is a person who uses their knowledge of computer systems and security vulnerabilities to gain unauthorized access to computer systems or networks. Unlike ethical hackers, who use their skills to identify and fix security flaws, crackers use their skills for malicious purposes, such as stealing sensitive information, damaging systems, or causing disruption to services.

Here's an example of how a cracker might operate:
Imagine a cracker wants to gain access to a company's network in order to steal sensitive customer data. The cracker begins by scanning the company's network for vulnerabilities, such as weak passwords or outdated software. Once a vulnerability is identified, the cracker may use an exploit, or a piece of software that takes advantage of the vulnerability to gain access to the network.
Once inside the network, the cracker may use various tools and techniques to move laterally across the network, looking for valuable data or other targets. The cracker may use social engineering tactics, such as phishing emails or fake websites, to trick employees into revealing sensitive information or providing access to the network.

The cracker may also use malware, such as keyloggers or remote access trojans, to gain persistent access to the network and continue stealing data or carrying out malicious activities.

Crackers can be highly skilled and difficult to detect, and can cause significant harm to organizations and individuals. To protect against crackers, it's important to implement strong security controls and access policies, keep software and systems up to date with the latest security patches, and train employees on how to identify and prevent social engineering attacks.

DoS: A Denial of Service (DoS) attack is a type of cyber attack in which an attacker attempts to disrupt normal traffic to a computer system, network, or website, making it unavailable to users. The goal of a DoS attack is to overload the targeted system with a flood of traffic or requests, causing it to crash or become unresponsive.

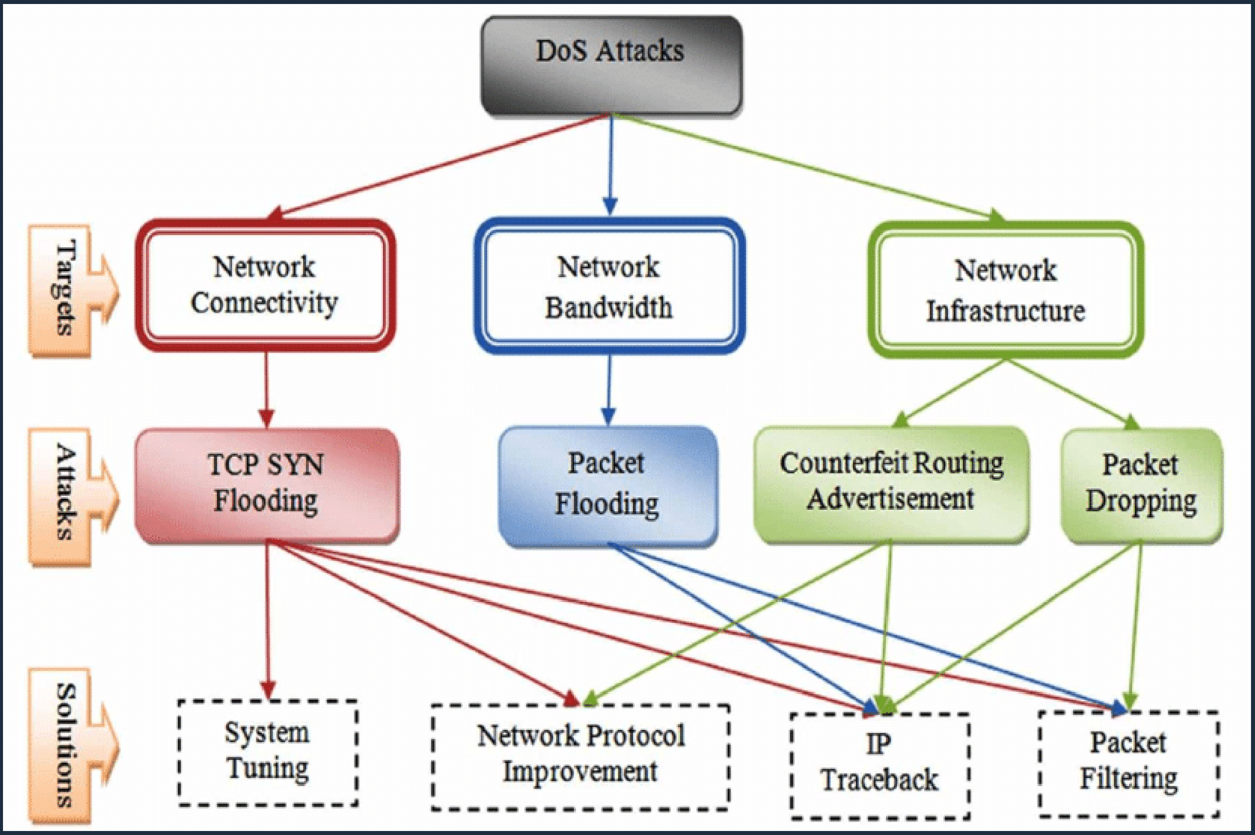

Denial-of-Service (DoS) Attack
In the most common example of Denial-of-Service (DoS) attacks, an attacker uses a network of hijacked computers.
This network is used to flood the target site with phony server requests, leaving no bandwidth for legitimate traffic.
HACKER
TARGET SERVER

Here's an example of how a DoS attack might work:

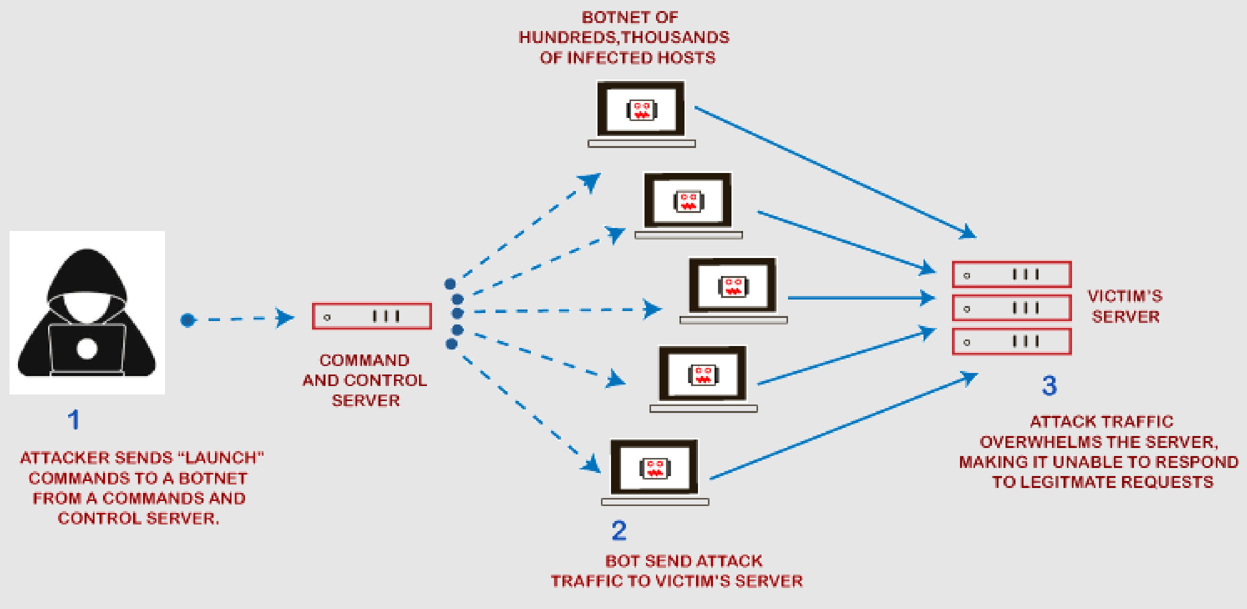
Imagine a company operates an online store that receives a large volume of traffic from customers every day. An attacker wants to disrupt the company's operations by taking down its website. The attacker uses a software tool called a botnet, which is a network of infected computers that can be controlled remotely, to flood the company's website with a huge amount of traffic, making it unavailable to customers.

The botnet can generate so much traffic that it overwhelms the company's servers, causing them to crash or become unresponsive. This makes it impossible for customers to access the website, place orders, or interact with the company.

DoS attacks can be highly effective at disrupting normal operations, and can cause significant damage to organizations and individuals. To protect against DoS attacks, it's important to implement security controls and access policies that limit the amount of traffic that can be sent to a system or website, as well as implementing measures to detect and mitigate attacks when they occur. This may include using firewalls, intrusion detection systems, or other security tools that can help identify and block malicious traffic.



DDoS: A Distributed Denial of Service (DDoS) attack is a type of cyber attack in which an attacker uses multiple compromised computers or devices to flood a targeted system or website with a huge amount of traffic or requests, overwhelming its servers and making it unavailable to users.

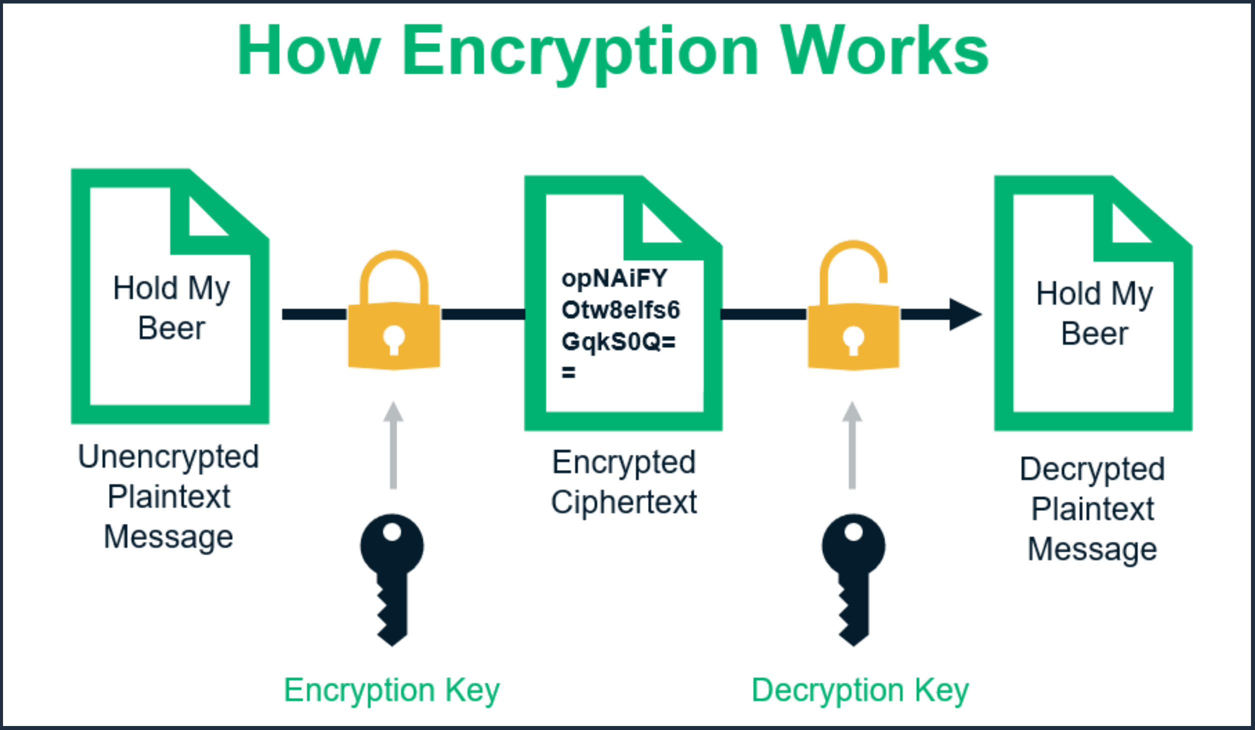


Here's an example of how a DDoS attack might work:
Imagine a company operates a popular gaming website that receives a large volume of traffic from players around the world. An attacker wants to disrupt the company's operations and make the website unavailable to players.
The attacker uses a botnet, which is a network of infected computers or devices that can be controlled remotely, to launch a DDoS attack on the company's website. The botnet consists of thousands or even millions of devices, such as home routers or Internet of Things (IoT) devices, that have been infected with malware and are under the control of the attacker.

The attacker commands the botnet to send a massive amount of traffic to the company's website, overwhelming its servers and making it unavailable to players. The sheer volume of traffic generated by the botnet can be enough to bring down even large-scale websites and services, causing significant damage to the targeted organization.

DDoS attacks are difficult to prevent and can be highly effective at disrupting normal operations. To protect against DDoS attacks, organizations can implement measures such as using content delivery networks (CDNs) to distribute traffic across multiple servers, implementing load balancing techniques to distribute traffic evenly across servers, and using intrusion prevention systems (IPS) or DDoS mitigation services to detect and mitigate attacks when they occur.

Encryption: Encryption is the process of converting plain text or data into a coded form that can be read only by authorized parties. Encryption is used to protect sensitive data, such as financial transactions, medical records, and personal information, from unauthorized access or theft.



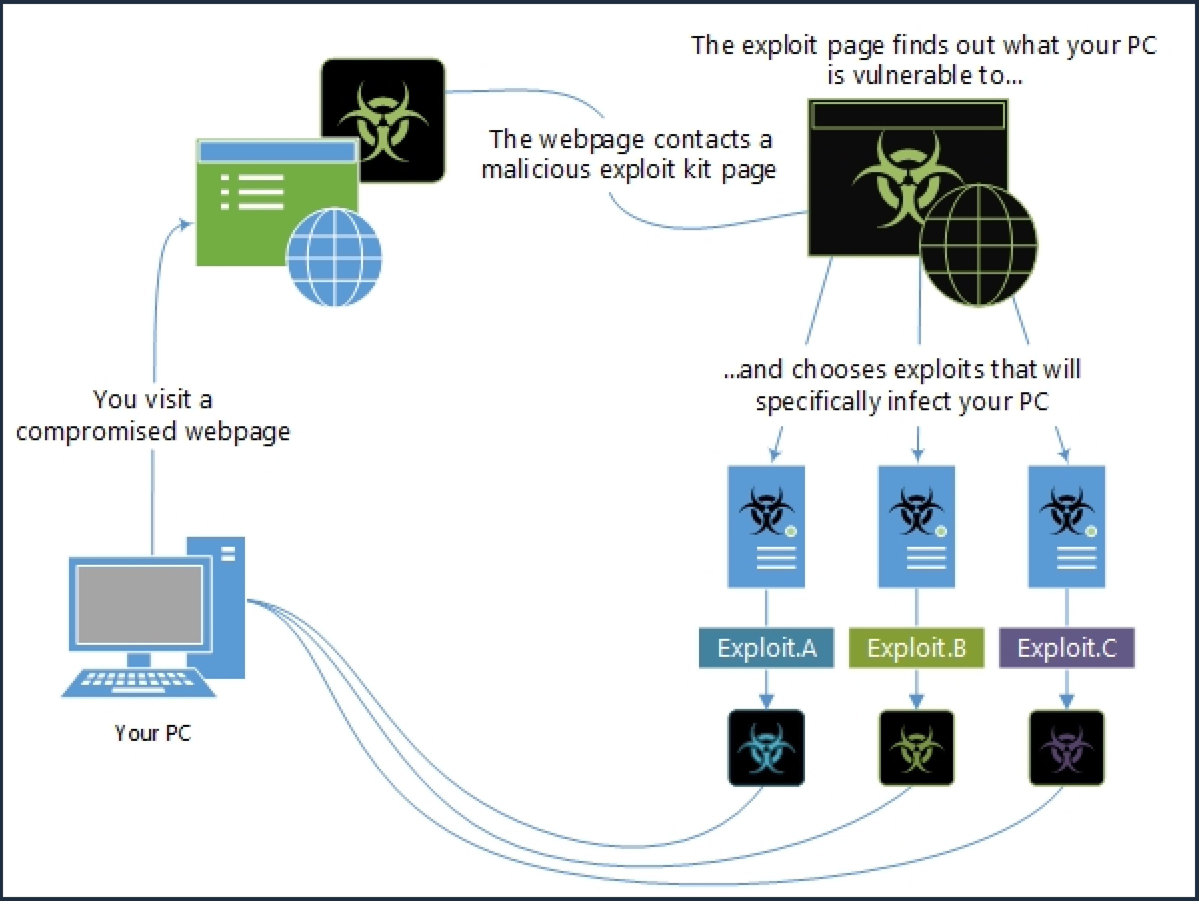
Here's an example of how encryption might work:
Imagine you want to send a confidential email to a colleague. You use an email encryption software, such as PGP or S/MIME, to encrypt the contents of the email before sending it.

The encryption software generates a unique digital key that is used to scramble the contents of the email. The key can only be decrypted by the intended recipient, who has a matching digital key that allows them to read the contents of the email in its original form.

When the email is received by the recipient, the encryption software uses the recipient's digital key to decrypt the contents of the email, making it readable. If the email is intercepted or stolen by a third party, they will not be able to read the contents of the email, as they do not have the matching digital key.
Encryption can be used to protect data in transit, such as email or online transactions, as well as data at rest, such as files stored on a computer or server. It

is an essential tool for protecting sensitive information and maintaining data privacy and security.

Exploit: An exploit is a type of cyber attack that takes advantage of a vulnerability or weakness in a computer system or software to gain unauthorized access or perform malicious actions. Exploits can be used to steal sensitive data, install malware, or take control of a system.


The exploit page finds out what your PC is vulnerable to...
The webpage contacts a malicious exploit kit page
You visit a compromised webpage
...and chooses exploits that will specifically infect your PC
Exploit.A
Exploit.B
Exploit.C
Your PC

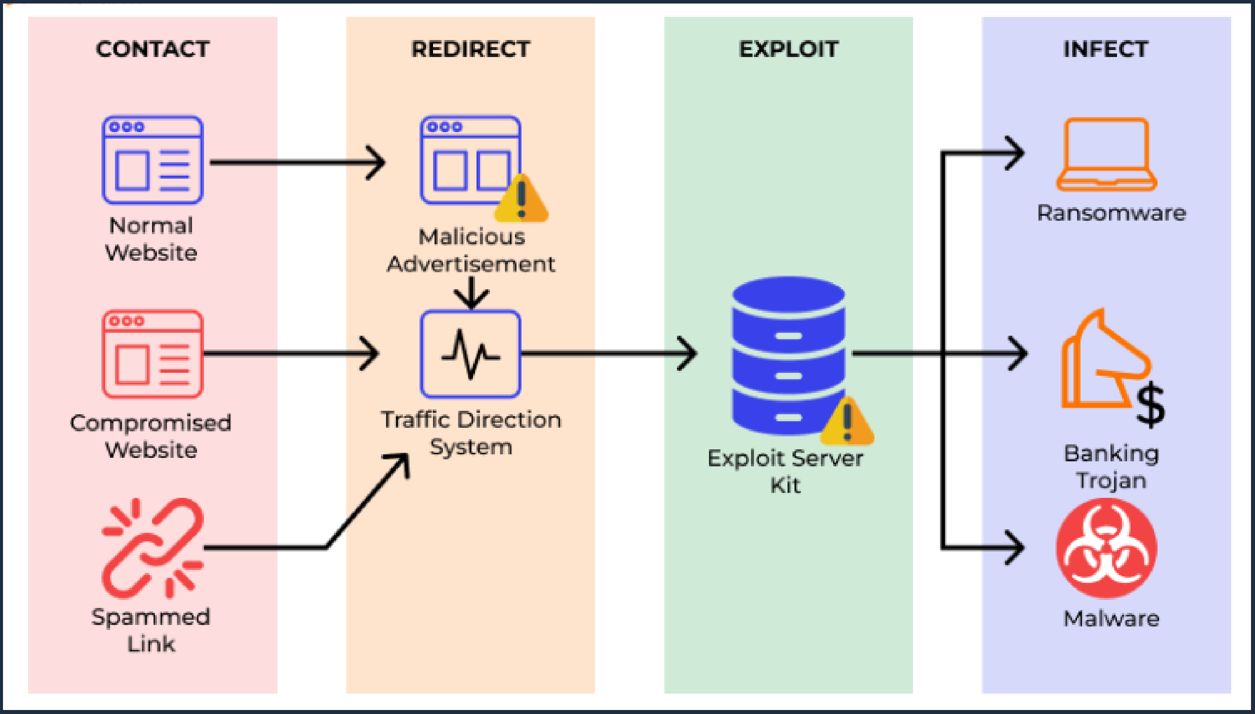
Here's an example of how an exploit might work:
Imagine a company uses a popular web application that has a known vulnerability that allows remote code execution. An attacker discovers this vulnerability and writes a piece of code called an exploit that takes advantage of the vulnerability to gain access to the company's servers.

The attacker sends the exploit to the web application, which executes the code and gives the attacker access to the system. With this access, the attacker can steal sensitive data, install malware, or carry out other malicious actions.

Exploits can be highly effective at compromising computer systems and networks, and can be difficult to detect and prevent. To protect against exploits, it's important to keep software and operating systems up-to-date with the latest security patches, use antivirus software and firewalls to detect and block attacks, and implement access controls and security policies that limit the amount of access that users and applications have to sensitive data and systems.

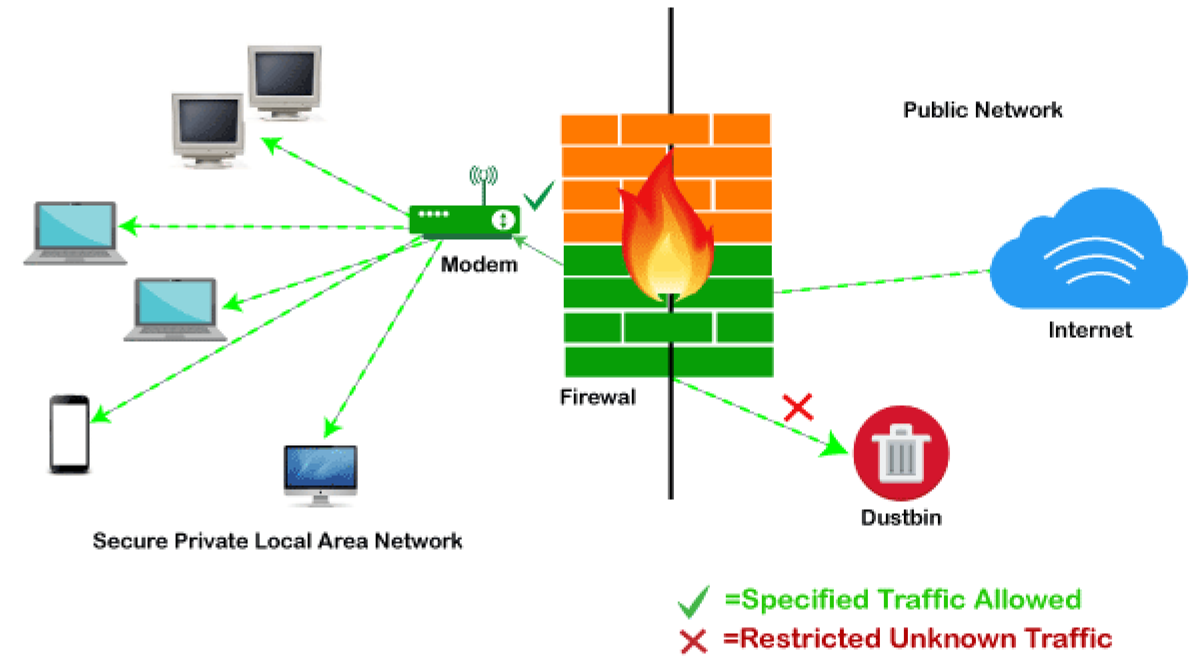
Exploit kit: An exploit kit is a type of malicious software that automates the process of delivering and executing exploits on a victim's computer or device.
Here's an example of how an exploit kit might work:
An attacker sets up an exploit kit on a website that appears to be legitimate or popular, such as a news or entertainment site. When a user visits the site, the exploit kit runs in the background, scanning the user's computer for vulnerabilities and weaknesses.

If the exploit kit finds a vulnerability, it automatically downloads and executes a malicious payload, such as ransomware, banking trojans, or other types of malware, without the user's knowledge or consent. This can result in a range of negative consequences, such as data theft, financial loss, or system compromise.
Exploit kits are often used in drive-by download attacks, in which a user is infected simply by visiting a compromised website or clicking on a malicious link. Because exploit kits can automate the process of finding and exploiting vulnerabilities, they are a popular tool for attackers looking to compromise large numbers of devices or systems.



To protect against exploit kits, it's important to keep software and operating systems up-to-date with the latest security patches, use antivirus software and firewalls to detect and block attacks, and be cautious when clicking on links or downloading files from unfamiliar or suspicious sources.

Firewall: A firewall is a network security device that monitors and filters incoming and outgoing network traffic based on an organization's previously established security policies. It is used to prevent unauthorized access to or from a network while allowing legitimate traffic to pass through.


Public Network
Modem
Internet
Firewal
Dustbin
Secure Private Local Area Network
✓ =Specified Traffic Allowed
✗ =Restricted Unknown Traffic

Here's an example of how a firewall might work:
Imagine a company has a network that is connected to the internet. To protect the network from outside threats, the company installs a firewall. The firewall is configured to allow traffic to and from certain IP addresses, ports, and protocols based on the company's security policies. For example, the firewall might be configured to block all incoming traffic except for web traffic on port 80.
When a user on the company's network tries to access a website on the internet, the request goes through the firewall. The firewall checks the request against its security policies and allows the request to pass through if it meets the criteria. If the request does not meet the criteria, the firewall blocks the request and prevents the user from accessing the website.

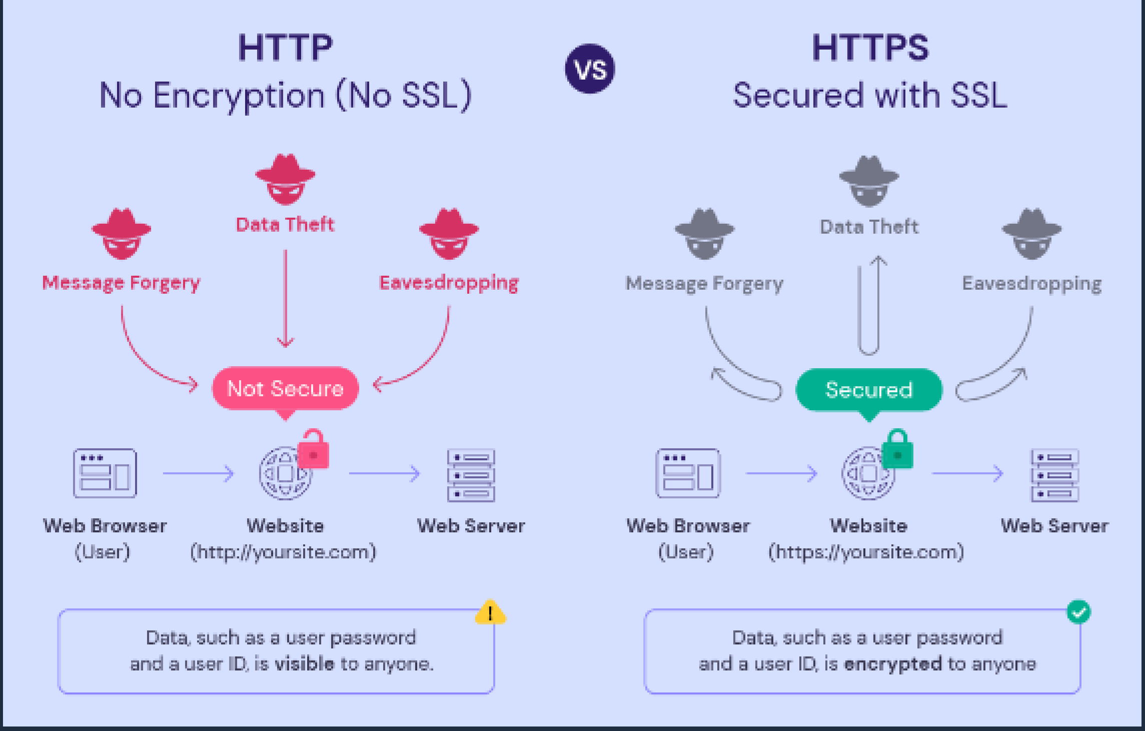
Firewalls can be hardware or software-based, and can be used to protect individual computers or entire networks. They are an essential tool for protecting against cyber attacks and maintaining network security.

HTTPS/SSL/TLS: HTTPS (Hypertext Transfer Protocol Secure) is a protocol for secure communication over the internet. It is used to encrypt and authenticate data transmitted between a web server and a client, such as a web browser, to protect against eavesdropping, tampering, and data theft.

SSL (Secure Sockets Layer) and TLS (Transport Layer Security) are the encryption protocols used to establish a secure connection between the server and the client. SSL and TLS use a combination of public key and symmetric key encryption to secure data transmission.

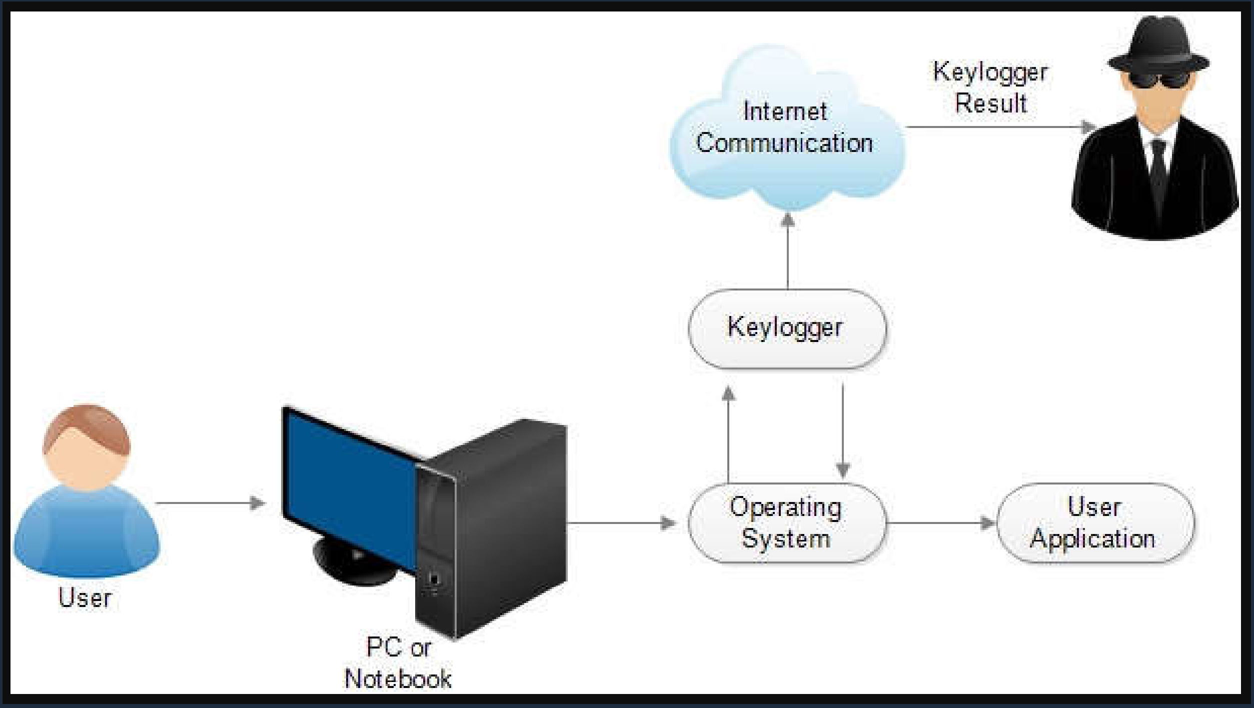
Here's an example of how HTTPS/SSL/TLS might work:
Imagine you want to buy something online from an e-commerce website. When you enter the website's URL in your web browser, the browser establishes a connection with the website's server using HTTPS.

The website's server sends a digital certificate to the browser to verify its identity. The browser checks the certificate to ensure that it is valid and issued by a trusted certificate authority (CA). If the certificate is valid, the browser generates a symmetric key, encrypts it with the server's public key, and sends it to the server. The server decrypts the symmetric key with its private key and uses it to encrypt all subsequent data transmitted between the server and the client. This ensures that the data cannot be intercepted or modified by attackers.
Throughout the session, the browser and server exchange encrypted data using SSL or TLS, and the browser displays a padlock icon in the address bar to indicate that the connection is secure.



By using HTTPS/SSL/TLS, online transactions and communications can be protected from interception, eavesdropping, and data theft, making it an essential component of online security.

Keystroke logging: Keystroke logging, also known as keylogging, is a technique used to monitor and record the keystrokes typed on a keyboard. Keystroke logging can be used for legitimate purposes, such as monitoring employee productivity, but it can also be used for malicious purposes, such as stealing passwords or sensitive information.

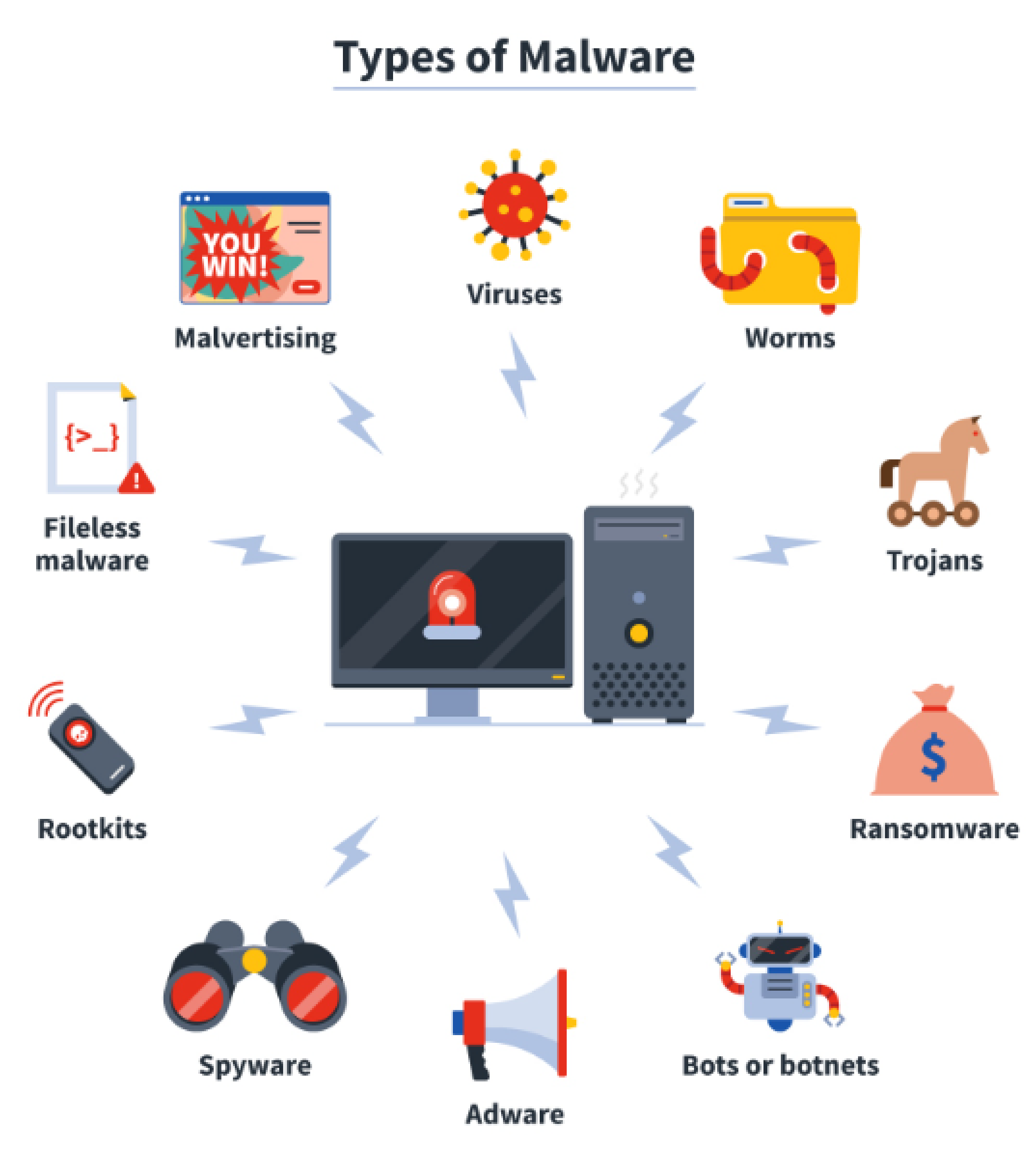


Here's an example of how keystroke logging might work:
An attacker installs a keystroke logger on a victim's computer or device, often through a phishing email or a malicious download. The keystroke logger runs in the background and records every keystroke typed by the victim, including passwords, credit card numbers, and other sensitive information.

The keystroke logger can send the recorded data to the attacker through various methods, such as email or a remote server. The attacker can then use this information for malicious purposes, such as identity theft or financial fraud.
To protect against keystroke logging, it's important to use anti-virus software and firewalls to detect and block malicious software, avoid clicking on suspicious links or

downloading files from untrusted sources, and use two-factor authentication to protect sensitive accounts.

Malware: Malware is short for "malicious software." It is a type of software designed to harm or exploit computers, devices, or networks. Malware can be used to steal sensitive information, corrupt or delete files, hijack computer resources, and more.



Here are a few examples of common types of malware:

- Virus: A virus is a type of malware that attaches itself to a legitimate program and replicates itself when the program is executed. Viruses can spread rapidly and cause damage to a computer or network.
- Trojan: A Trojan, also known as a Trojan horse, is a type of malware that disguises itself as a legitimate program but contains malicious code. Trojans can be used to steal sensitive information, such as passwords or credit card numbers, or to provide remote access to a computer or network.
- Ransomware: Ransomware is a type of malware that encrypts a victim's files and demands payment in exchange for the decryption key. Ransomware attacks have become increasingly common in recent years and can cause significant financial and reputational damage.
- Spyware: Spyware is a type of malware that is designed to gather information from a victim's computer or device without their knowledge or consent. Spyware can be used to monitor a victim's internet activity, steal personal information, or display unwanted ads.

To protect against malware, it's important to use up-to-date anti-virus software and firewalls, avoid clicking on suspicious links or downloading files from untrusted sources, and keep software and operating systems updated with the latest security patches.

Payload: In the context of computer security, a payload refers to the part of a malware program that is designed to cause harm or achieve a specific malicious goal. Payloads can take many forms and can include any type of malicious action, such as stealing data, damaging files, or hijacking a system.

Here are a few examples of payloads that can be used by malware:

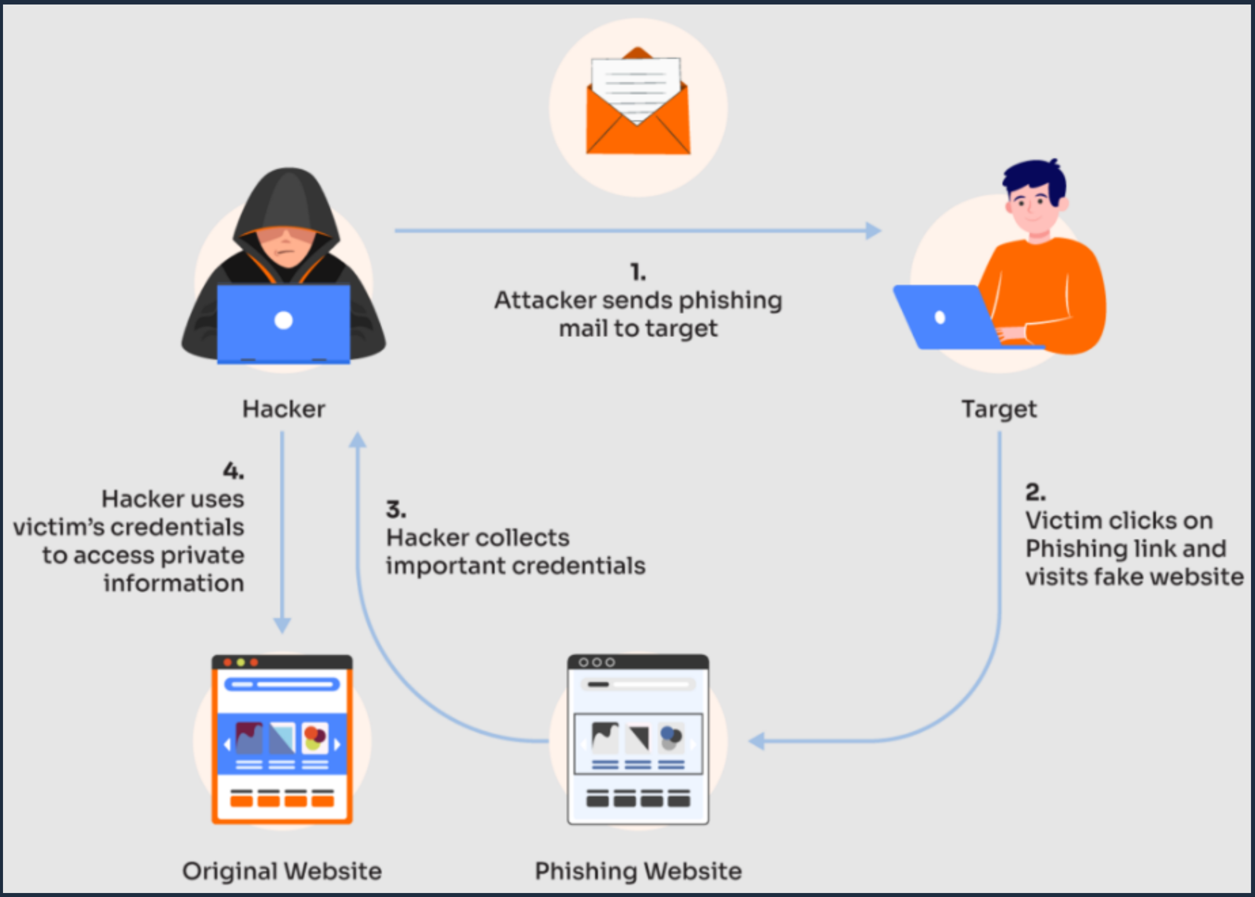
- Remote Access Trojans (RATs): RATs are a type of malware that allows an attacker to gain remote access to a victim's computer or device. The payload for a RAT might include keylogging software, screen capture tools, or remote control tools.
- Cryptojacking: Cryptojacking is a type of malware that uses a victim's computer or device to mine cryptocurrency without their knowledge or consent. The payload for a cryptojacking attack might include mining software and scripts that run in the background.
- Ransomware: As mentioned earlier, ransomware is a type of malware that encrypts a victim's files and demands payment in exchange for the

decryption key. The payload for a ransomware attack might include the encryption software and a demand message to the victim.

- Botnets: Botnets are networks of infected computers that are controlled by a central attacker. The payload for a botnet might include software to allow the attacker to remotely control the infected machines, send spam emails, or launch DDoS attacks.

To protect against payloads, it's important to use up-to-date anti-virus software and firewalls, avoid clicking on suspicious links or downloading files from untrusted sources, and keep software and operating systems updated with the latest security patches.

Phishing: Phishing is a type of cyber attack in which an attacker attempts to trick a victim into providing sensitive information, such as login credentials or credit card numbers, by disguising themselves as a trustworthy entity. Phishing attacks can take many forms, but they often involve emails, text messages, or websites that are designed to look like they are from a legitimate source.

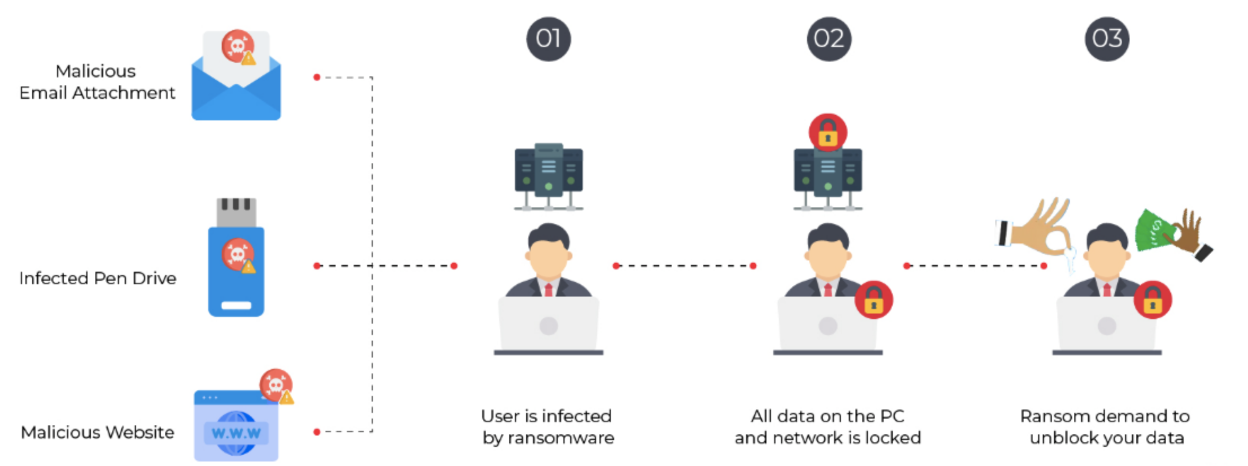

1.
Attacker sends phishing mail to target
Hacker
Target
4.
Hacker uses victim's credentials to access private information
3.
Hacker collects important credentials
2.
Victim clicks on Phishing link and visits fake website
Original Website
Phishing Website

Here's an example of how a phishing attack might work:

- The attacker sends an email to the victim that appears to be from a trusted entity, such as a bank or social media site. The email may contain a message that prompts the victim to take action, such as updating their account information or resetting their password.
- The email may include a link to a fake website that looks like the legitimate site, but is actually controlled by the attacker. The victim may be prompted to enter their login credentials or other sensitive information on this site.
- Once the victim has provided their information, the attacker can use it to gain access to the victim's accounts, steal their identity, or commit other types of fraud.

To protect against phishing attacks, it's important to be vigilant and to follow best practices for online security. This includes being cautious of unsolicited emails or messages, verifying the legitimacy of websites and login pages, and never providing sensitive information to an untrusted source. Organizations can also use email filters and anti-phishing software to help detect and prevent phishing attacks.

Ransomware: Ransomware is a type of malware that encrypts a victim's files or blocks access to their system, and then demands a ransom payment in exchange for the decryption key or access to the system. Ransomware attacks can be devastating, as they can result in the loss of important data and the disruption of critical systems.


Malicious Email Attachment
Infected Pen Drive
Malicious Website
W.W.W
01
02
03
User is infected by ransomware
All data on the PC and network is locked
Ransom demand to unblock your data

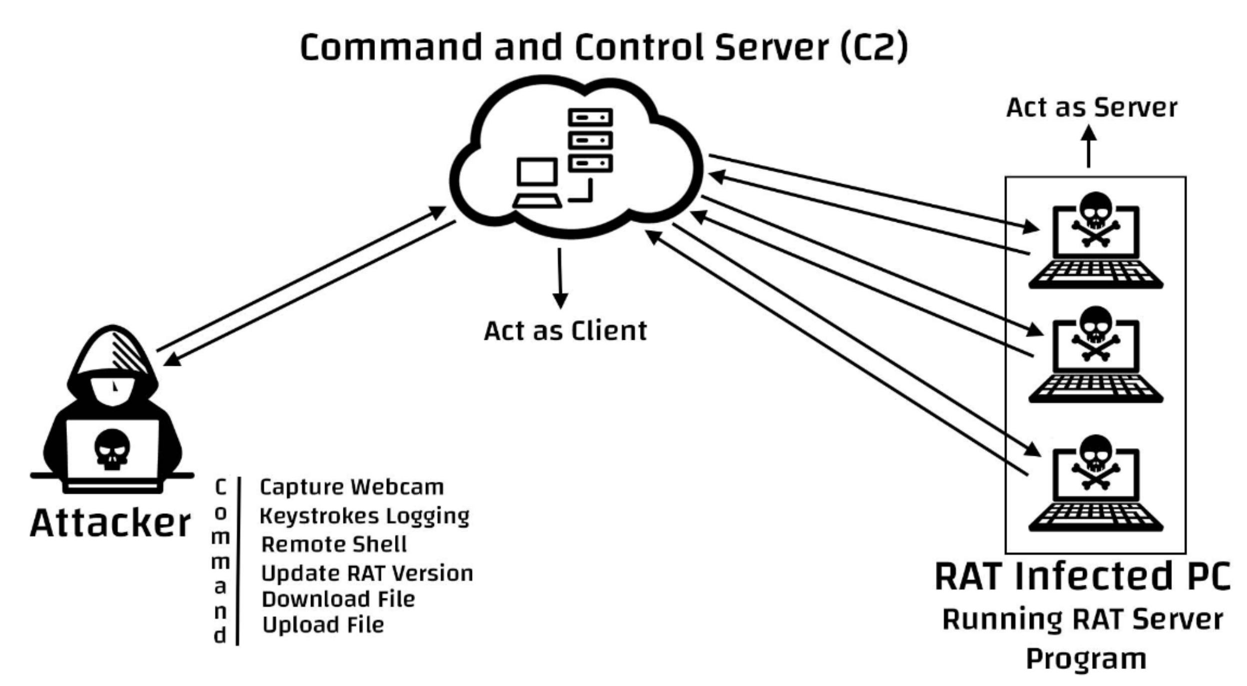
Here's an example of how a ransomware attack might work:

- The victim receives an email with a malicious attachment or link, or they visit a compromised website that contains malware.
- The malware downloads and installs on the victim's computer, encrypting their files and preventing access to their system.
- The attacker demands payment in exchange for the decryption key or access to the system. They may leave a message on the victim's computer or provide instructions on how to pay the ransom.
- If the victim pays the ransom, the attacker may provide the decryption key or unlock the victim's system. However, there is no guarantee that the attacker will honor their end of the bargain, and paying the ransom only encourages further attacks.

Some notable examples of ransomware attacks include the WannaCry attack that targeted computers running Windows in 2017, the Petya/NotPetya attack in 2017 that affected companies worldwide, and the Colonial Pipeline ransomware attack in 2021 that disrupted the fuel supply to much of the eastern United States.

To protect against ransomware attacks, it's important to keep software and operating systems updated with the latest security patches, use anti-virus software and firewalls, and backup important data regularly to prevent loss in the event of an attack. It's also important to be cautious of unsolicited emails or messages, and to avoid clicking on suspicious links or downloading files from untrusted sources.

RAT: RAT stands for Remote Access Trojan, which is a type of malware that allows an attacker to take control of a victim's computer remotely. Once a RAT infects a computer, the attacker can use it to perform a variety of malicious activities, such as stealing sensitive information, spying on the victim, or using the victim's computer as a part of a larger botnet.



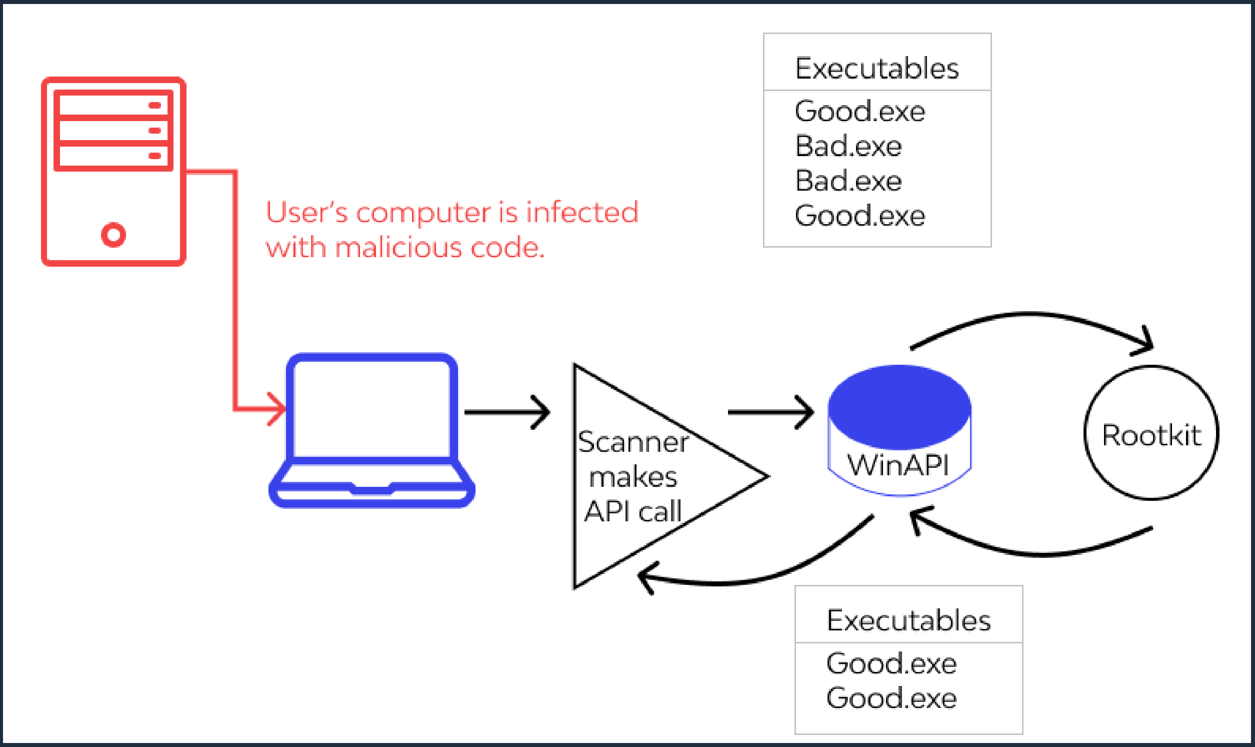
Here's an example of how a RAT attack might work:

- The victim receives an email with a malicious attachment or link, or they visit a compromised website that contains malware.
- The malware downloads and installs on the victim's computer, allowing the attacker to take control of the system remotely.
- The attacker can use the RAT to perform a variety of malicious activities, such as stealing login credentials, monitoring the victim's activity, or installing additional malware.
- The attacker can also use the RAT to access the victim's files and system resources, which can be used for further attacks or to steal sensitive information.

Some notable examples of RAT attacks include the Poison Ivy RAT that was used in targeted attacks against government agencies and defense contractors, and the DarkComet RAT that was used in attacks against Syrian activists.

To protect against RAT attacks, it's important to keep software and operating systems updated with the latest security patches, use anti-virus software and firewalls, and avoid downloading files or opening attachments from untrusted sources. It's also important to be cautious of unsolicited emails or messages, and to avoid clicking on suspicious links or downloading files from untrusted sources.

Rootkit: A rootkit is a type of malicious software that allows an attacker to gain privileged access to a victim's computer system, often hiding its presence from the victim and from security software. Once a rootkit has been installed, an attacker can use it to perform a variety of malicious activities, such as stealing sensitive information, installing additional malware, or controlling the victim's computer remotely.



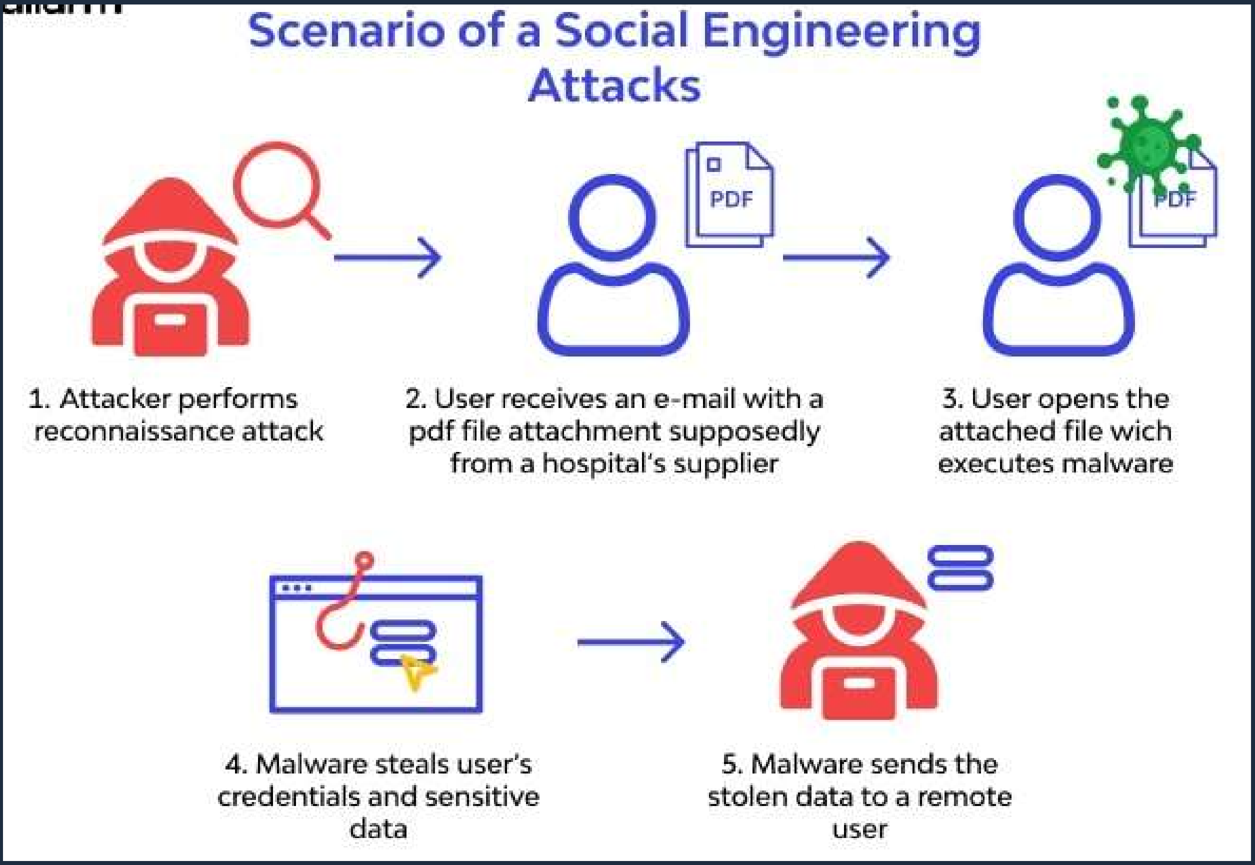
Here's an example of how a rootkit attack might work:

- The victim downloads and installs a program from a website or email attachment that contains a rootkit.
- The rootkit is installed on the victim's computer, often disguising its presence and avoiding detection by security software.
- The rootkit gives the attacker privileged access to the victim's computer system, allowing them to perform a variety of malicious activities.
- The attacker can use the rootkit to hide their activities, such as deleting log files or modifying system settings.

Some notable examples of rootkit attacks include the Sony BMG rootkit scandal in 2005, where Sony used a rootkit to hide its copy protection software on customers' computers, and the Stuxnet worm in 2010, which used a rootkit to infect and damage industrial control systems in Iran.

To protect against rootkit attacks, it's important to keep software and operating systems updated with the latest security patches, use anti-virus software and firewalls, and be cautious of downloading files or opening attachments from untrusted sources. It's also important to regularly scan your computer for rootkits using specialized tools designed to detect and remove them.

Social engineering: Social engineering is a type of cyber attack that relies on psychological manipulation to trick people into revealing sensitive information or performing actions that are not in their best interest. Social engineering attacks can take many forms, including phishing emails, phone calls, or even in-person interactions.


Scenario of a Social Engineering Attacks
PDF
PDF
1. Attacker performs reconnaissance attack
2. User receives an e-mail with a pdf file attachment supposedly from a hospital's supplier
3. User opens the attached file wich executes malware
4. Malware steals user's credentials and sensitive data
5. Malware sends the stolen data to a remote user

Here's an example of a social engineering attack:

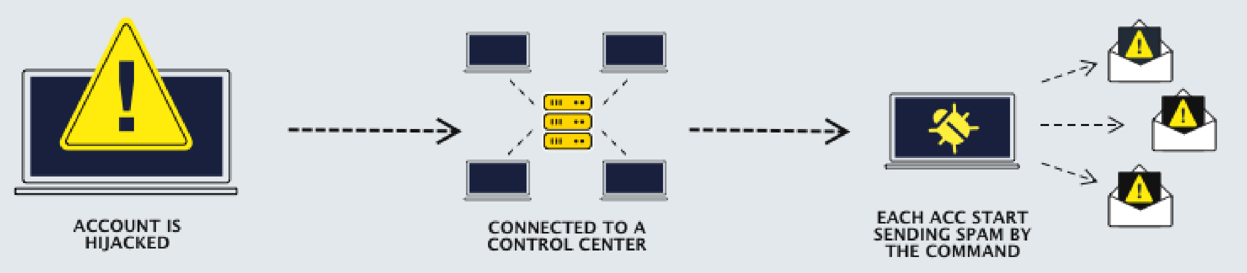
- An attacker sends a phishing email to a company's employees, posing as a legitimate business or service provider and requesting that the employee provide their login credentials or other sensitive information.

- The employee, thinking that the email is legitimate, provides the requested information.
- The attacker can now use the information to access the company's systems and steal sensitive information or install malware.

Other examples of social engineering attacks might include an attacker posing as a security researcher and requesting access to sensitive information or a hacker impersonating a tech support representative and convincing a victim to install malware.

To protect against social engineering attacks, it's important to educate employees and individuals about the tactics that attackers use, and to encourage them to be cautious of unsolicited emails, phone calls, or requests for sensitive information. It's also important to implement security policies and procedures that require verification of requests for sensitive information or changes to system settings, and to use multi-factor authentication to reduce the risk of stolen login credentials.

Spam: Spam refers to unsolicited or unwanted messages that are sent in bulk, often for the purpose of advertising or spreading malware. Spam can take many forms, including email spam, text message spam, and social media spam.


ACCOUNT IS HIJACKED
CONNECTED TO A CONTROL CENTER
EACH ACC START SENDING SPAM BY THE COMMAND

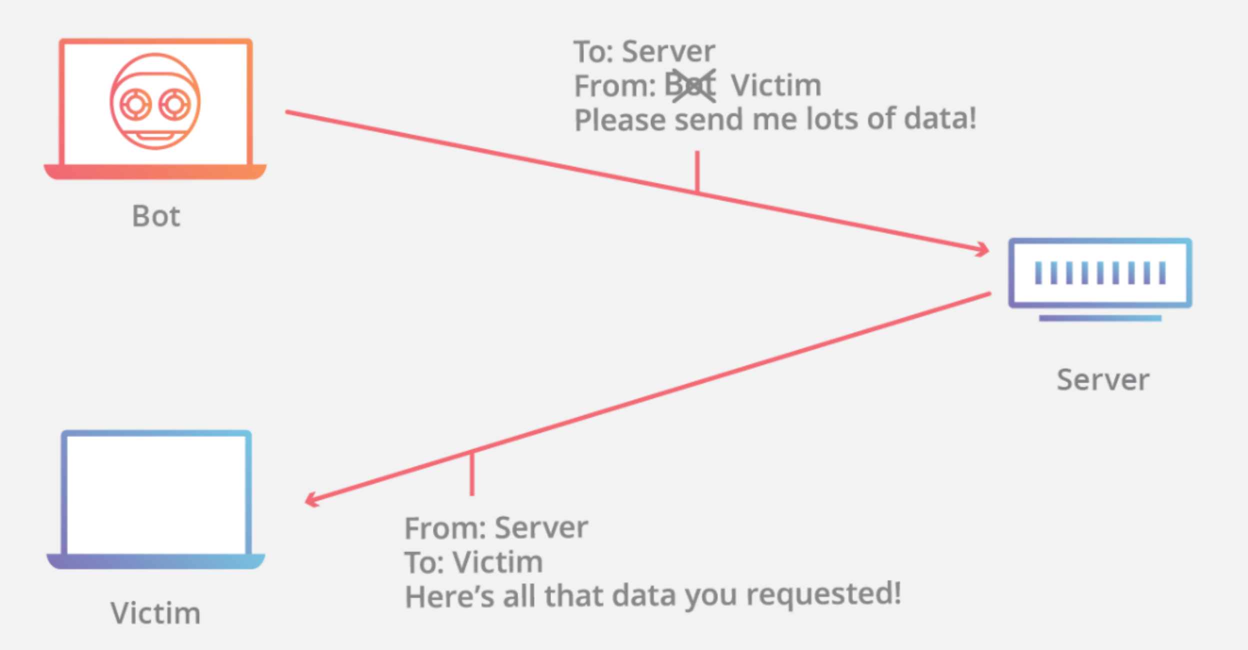
Here's an example of email spam:

- An attacker creates a list of email addresses, either by scraping them from websites or purchasing them from a third-party.
- The attacker sends out a large number of unsolicited emails, often advertising a product or service, or containing a malicious link or attachment.
- The recipient may be tricked into clicking on the link or opening the attachment, which can result in malware being installed on their computer or their personal information being stolen.

Other examples of spam might include text message spam, where an attacker sends unsolicited text messages to a large number of phone numbers, or social media spam, where an attacker creates fake accounts or bots to post spammy messages or links on social media platforms.

To protect against spam, it's important to use spam filters in your email and messaging software, and to be cautious of unsolicited messages from unknown senders. It's also important to avoid clicking on links or opening attachments in suspicious emails, and to use anti-virus software and firewalls to protect against malware.

Spoofing: Spoofing refers to a type of cyber attack where an attacker impersonates a legitimate person, device, or system in order to deceive the victim and gain access to sensitive information or systems. Spoofing attacks can take many forms, including email spoofing, IP spoofing, and caller ID spoofing.



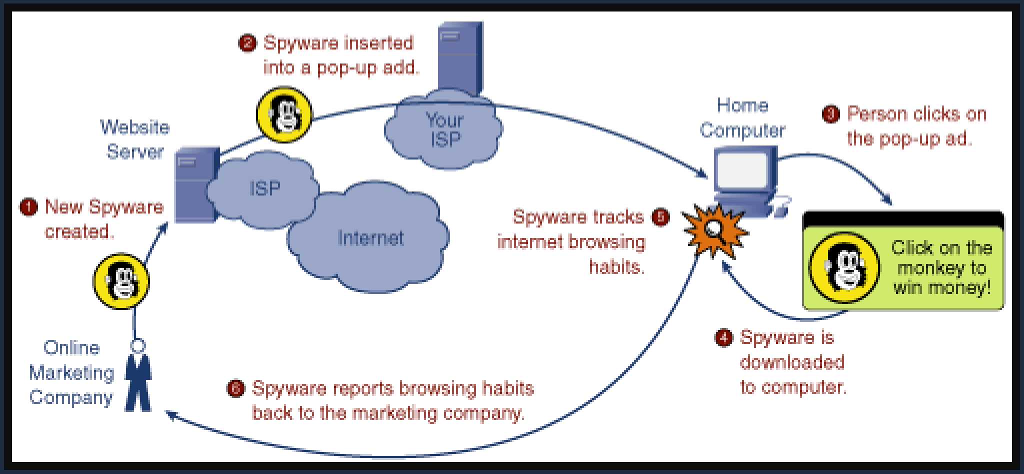
Here's an example of email spoofing:

- An attacker creates a fake email that appears to be from a legitimate company or organization, such as a bank or an e-commerce website.
- The attacker changes the "from" address in the email to make it appear as if the email is coming from the legitimate company or organization.
- The attacker sends the email to the victim, requesting that they provide sensitive information, such as login credentials or credit card numbers.
- The victim, thinking that the email is legitimate, provides the requested information.

Other examples of spoofing might include IP spoofing, where an attacker modifies the source IP address of a packet in order to hide their identity or impersonate another system, or caller ID spoofing, where an attacker manipulates the caller ID information on a phone call in order to appear as if they are calling from a different number.

To protect against spoofing attacks, it's important to be cautious of unsolicited messages or requests for sensitive information, and to verify the identity of the sender or caller through independent means, such as by calling a known phone number or visiting a verified website. It's also important to use security tools and protocols, such as two-factor authentication, to reduce the risk of stolen login credentials or identity theft.

Spyware: Spyware is a type of malware that is designed to secretly gather information from a computer or device without the user's knowledge or consent. The information that is gathered may include keystrokes, web browsing history, login credentials, and other sensitive data, which can then be used for malicious purposes such as identity theft or corporate espionage.



2 Spyware inserted into a pop-up add.
Website Server
Your ISP
ISP
Internet
Home Computer
3 Person clicks on the pop-up ad.
1 New Spyware created.
Spyware tracks internet browsing habits. 5
Click on the monkey to win money!
4 Spyware is downloaded to computer.
Online Marketing Company
6 Spyware reports browsing habits back to the marketing company.

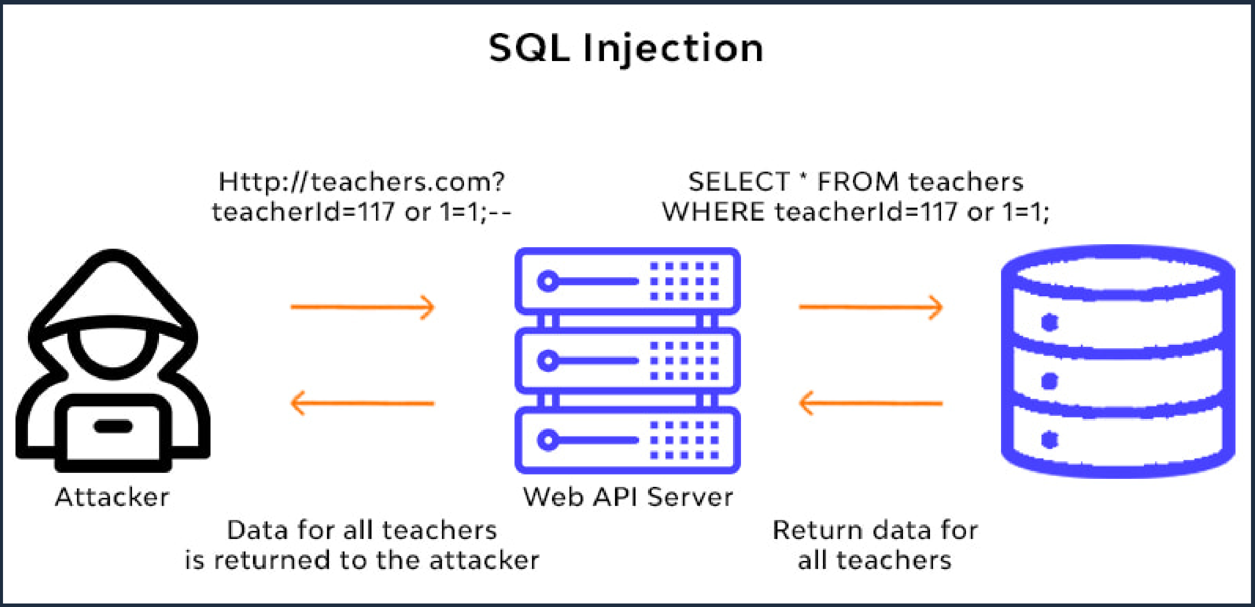
Here's an example of spyware:

- A user downloads a free software application from an untrusted source.
- The software application contains spyware code that is installed on the user's computer without their knowledge.
- The spyware begins to gather information from the user's computer, such as their browsing history and login credentials.
- The spyware sends this information back to a remote server controlled by the attacker, who can then use the information for malicious purposes.

Other examples of spyware might include keyloggers, which record keystrokes in order to capture sensitive information such as passwords and credit card numbers, or adware, which displays unwanted advertisements and tracks the user's browsing habits in order to deliver targeted ads.

To protect against spyware, it's important to use reputable antivirus and anti-malware software, and to avoid downloading software or opening email attachments from untrusted sources. It's also important to keep software and operating systems up to date with the latest security patches, as attackers often exploit vulnerabilities in older software versions to install spyware and other malware.

SQL Injection: SQL injection is a type of cyber attack that exploits vulnerabilities in web applications to manipulate the underlying database. The attack involves inserting malicious SQL code into a web form or other input field in order to gain unauthorized access to sensitive data, modify or delete data, or execute other malicious actions.



Here's an example of SQL injection:

- A user visits a vulnerable web application that uses SQL to retrieve data from a database.
- The user enters malicious SQL code into a web form or other input field, such as a search bar.

- The web application fails to properly sanitize or validate the user input, allowing the malicious SQL code to be executed by the database.
- The attacker is able to extract sensitive data from the database, such as login credentials or credit card numbers, or to modify or delete data stored in the database.

Other examples of SQL injection might include using SQL commands to execute arbitrary code on the underlying server, or to gain unauthorized access to administrative functions or other sensitive areas of the web application.

To protect against SQL injection attacks, it's important to follow secure coding practices, such as using parameterized queries or prepared statements to prevent untrusted input from being executed as SQL code. It's also important to regularly test web applications for vulnerabilities, and to keep software and systems up to date with the latest security patches.

Threat: A threat is any potential danger or risk that could cause harm or damage to a system, organization, or individual. In the context of cybersecurity, a threat refers to any malicious activity or attack that could compromise the security of a system or data.

Here's an example of a threat:

- A user receives an email from an unknown sender that contains a suspicious attachment.
- The user opens the attachment, which contains malware that infects their computer.
- The malware begins to harvest sensitive data from the user's computer, such as login credentials and credit card numbers.
- The attacker is able to use this data to steal money or commit identity theft.

Other examples of threats might include phishing attacks, in which attackers use social engineering tactics to trick users into revealing sensitive information or clicking on malicious links, or ransomware attacks, in which attackers encrypt a victim's data and demand payment in exchange for the decryption key.

To protect against threats, it's important to follow best practices for cybersecurity, such as using strong passwords, keeping software and systems up to date with the latest security patches, and using antivirus and anti-malware software. It's also important to remain vigilant and to report any suspicious activity to the appropriate authorities.