Common Cyberattacks

Attacks That Cause Damage

Attackers Intentionally Inflict Damage: Some cyberattacks are designed to directly harm victims, rather than steal data or money.

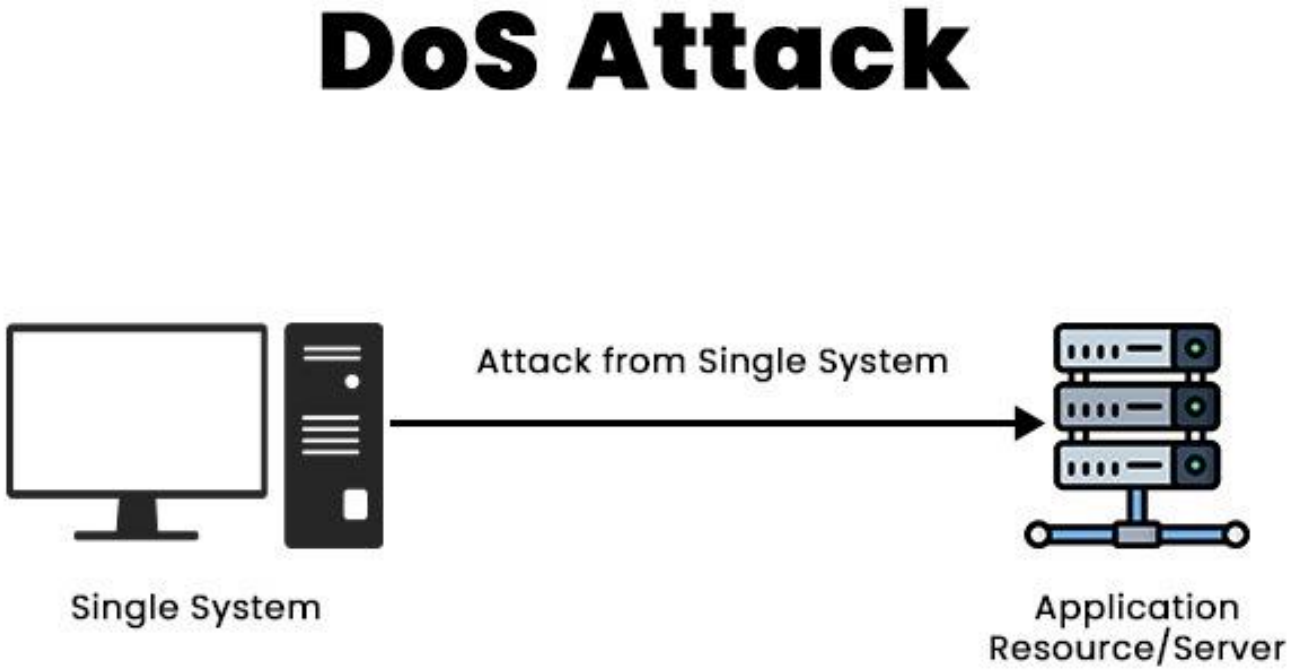
Diverse Forms of Harm: These attacks can cause financial, military, political, physical, or other types of damage, potentially benefiting the attacker.

Types of attacks that inflict damage include

- Denial-of-service (DoS) attacks
- Distributed denial-of-service (DDoS) attacks
- Botnets and zombies
- Data destruction attacks

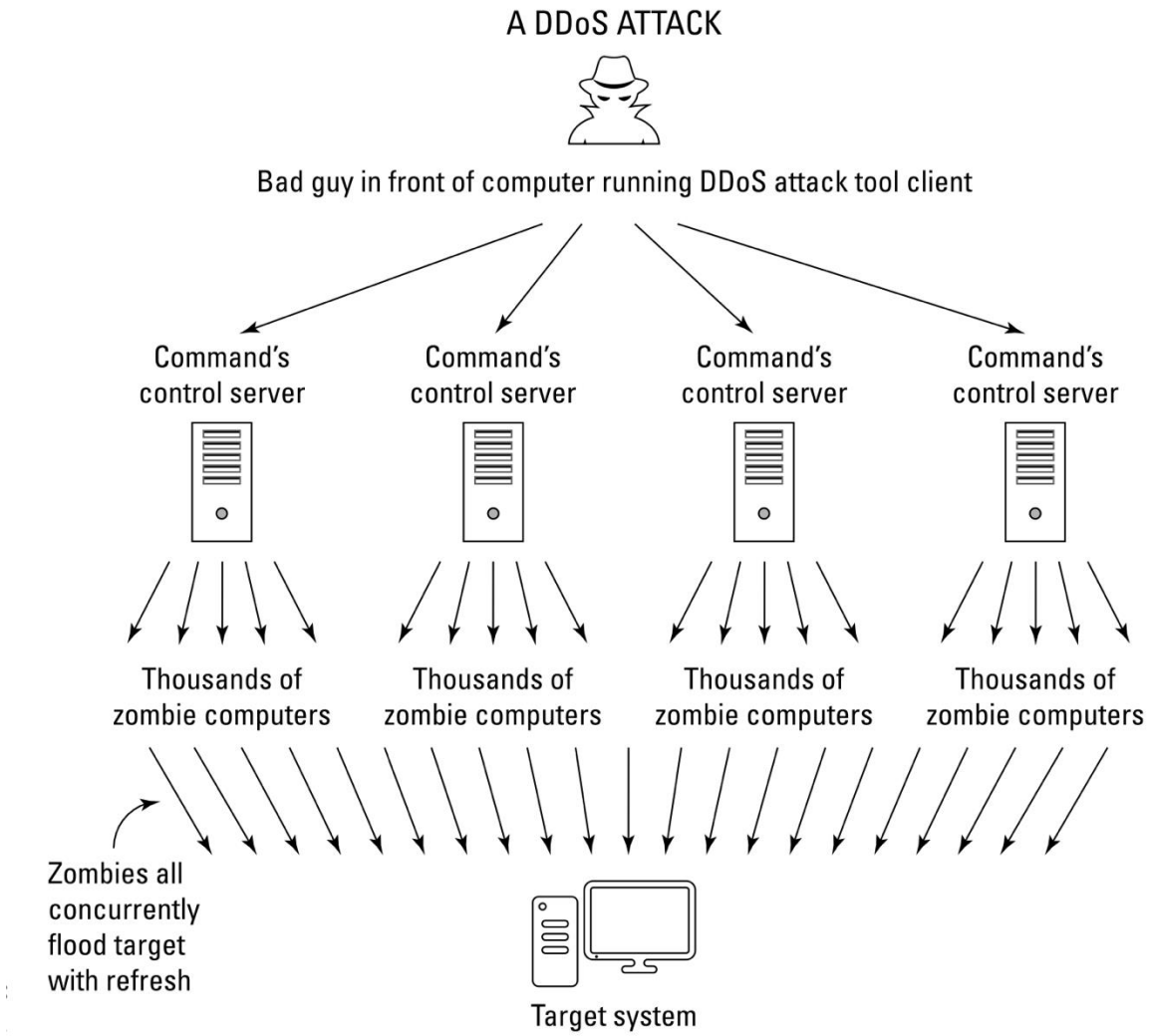
Denial-of-service (DoS) attacks

- Denial-of-service (DoS) attacks intentionally overload computers or networks with requests/data, hindering their ability to respond to legitimate users.
- Attackers may use normal or specially crafted requests to maximize the attack's impact.
- DoS attacks overwhelm **CPU**, **memory**, **network bandwidth**, or **networking infrastructure resources**.



Distributed denial-of-service (DDoS) attacks

- A distributed denial-of-service (DDoS) attack is a DoS attack carried out by numerous computers/devices across different locations simultaneously.
- DDoS attacks are now commonly distributed and can utilize devices beyond traditional computers, such as Internet-connected cameras.
- The primary goal of a DDoS attack is to knock the victim's system offline.
- Motivations for DDoS attacks include financial gain (harming competitors) and political objectives (silencing opponents).
- DDoS-for-hire services are available on the dark web, and hacktivists also use DDoS attacks to target sites for perceived injustices.



DDoS attacks can impact

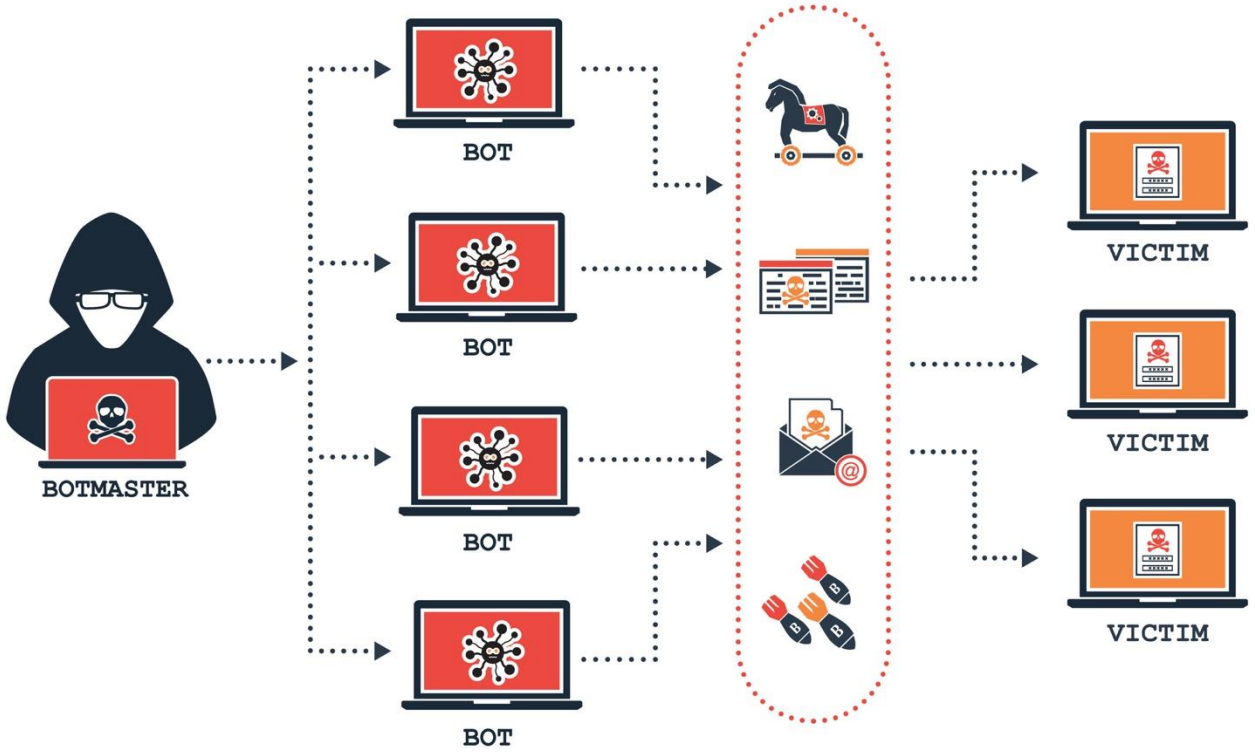
A DDoS attack on a local network can significantly **slow down all Internet access** from that network.

A DDoS attack can **render inaccessible a site** that a person plans on using.

A DDoS attack can lead users to obtain information **from one site instead of another**.

Botnets and zombies

- DDoS attacks frequently utilize botnets: collections of compromised computers (zombies) controlled remotely by attackers.
- These botnets consist of machines infected with malware, allowing attackers to use them without the owners' knowledge.
- Attackers can leverage these large networks to generate massive traffic, overwhelming the target server.



Data destruction attacks

- Data destruction attacks aim to damage victims by destroying or corrupting information and systems, going beyond temporary disruption.
- Motivations mirror those of DDoS attacks, with the added incentive of punishing non-compliance, such as refusing to pay a ransomware demand.
- Wiper attacks utilize malware to irrecoverably wipe data from storage devices, leading to significant data and software loss if backups are absent.

Impersonation

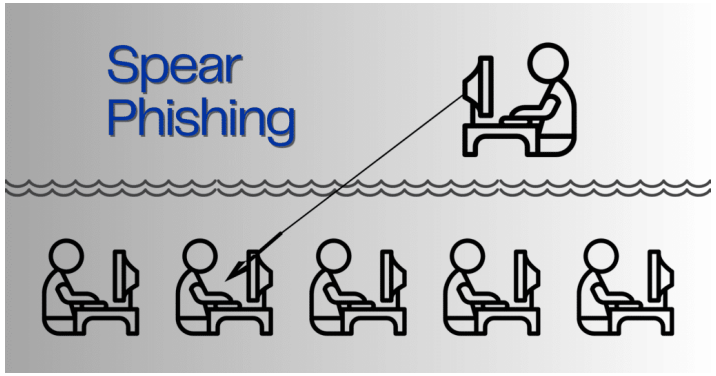
- The Internet significantly eases impersonation, enabling malicious actors to mimic legitimate entities like banks or stores.
- While physical mail and phone calls were used previously, the Internet provides a far more powerful platform for online impersonation.
- Creating convincing fake websites that closely resemble those of legitimate organizations is relatively quick and easy.
- Spoofing email addresses is also simple, allowing criminals to perpetuate various online scams and crimes through impersonation.

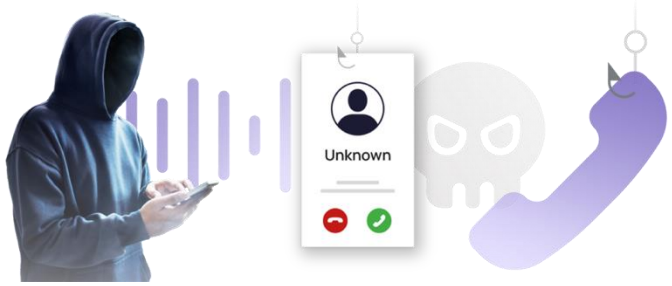
Phishing

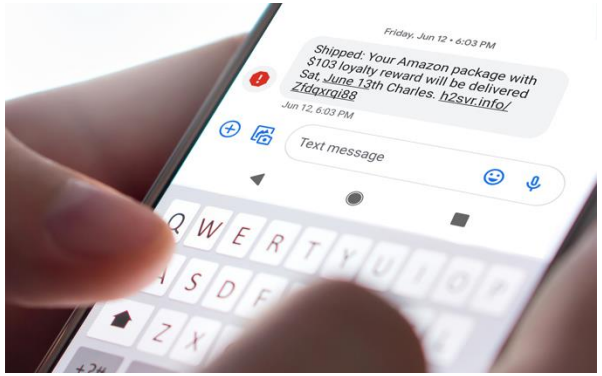
- A phishing attack occurs when a hacker poses as a legitimate entity to steal private information.
- A common example is a fake email from a bank urging users to click a link and reset their password, leading to a replica website designed to steal login credentials.
- Despite being a long-standing threat, phishing attacks remain prevalent, with many businesses experiencing successful breaches annually.

Types of Phishing

- **Spear Phishing**: Highly personalized emails target specific individuals. The hacker pretends to be a trusted entity and asks the victim to click a link or perform an action, which may lead to malware downloads.
- **Vishing (Voice Phishing)**: The hacker calls the victim, posing as a legitimate organization like your bank. They may use caller ID spoofing to appear trustworthy.
- **SMiShing (SMS Phishing)**: Cyber criminals send phishing messages via text.



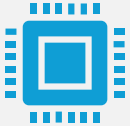




Interception

INTERCEPTION TARGETS DATA IN TRANSIT: ATTACKERS CAPTURE DATA AS IT'S TRANSMITTED BETWEEN DEVICES OR PEOPLE AND DEVICES.

UNENCRYPTED DATA IS VULNERABLE: INTERCEPTED UNENCRYPTED DATA CAN BE READILY MISUSED BY ATTACKERS.

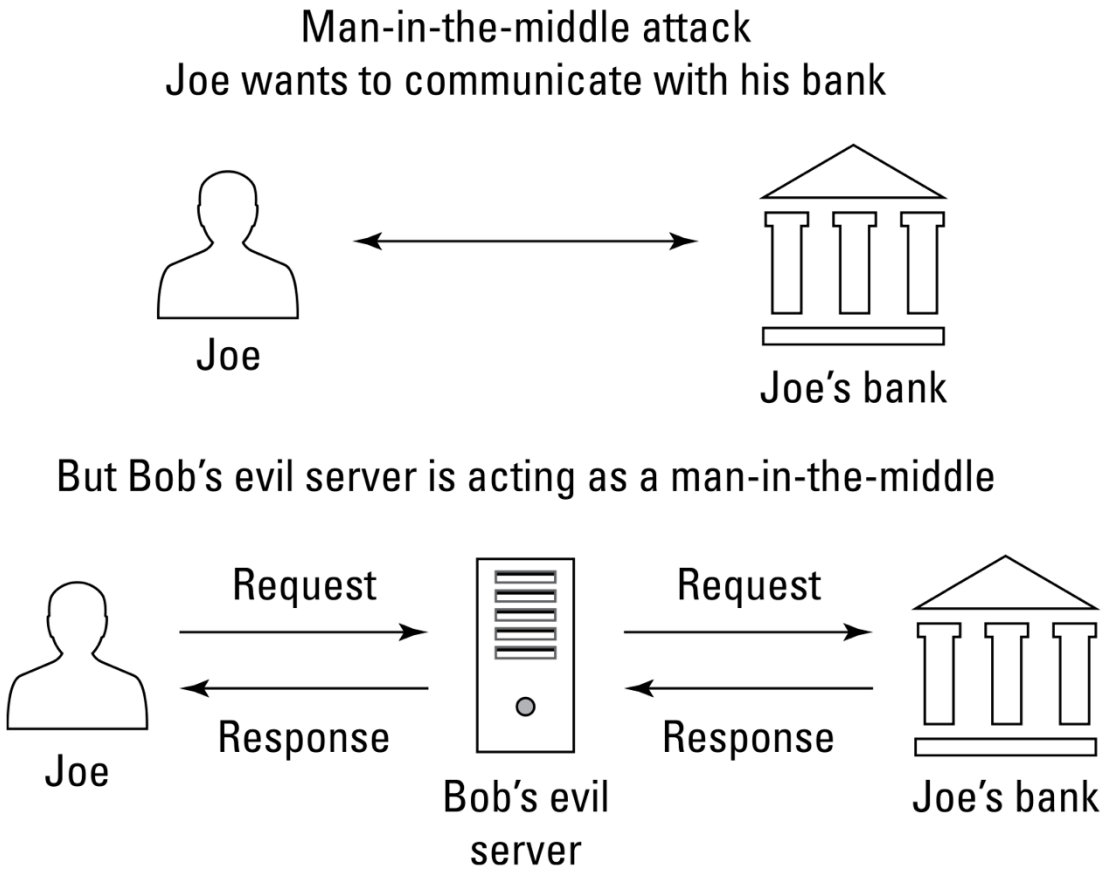


HUMAN-GENERATED DATA IS OFTEN UNPROTECTED: DATA DIRECTLY FROM HUMANS (E.G., VOICE RECORDINGS) IS FREQUENTLY UNENCRYPTED.

FUTURE THREATS TO ENCRYPTED DATA: EVEN STRONG ENCRYPTION MAY BECOME INEFFECTIVE IN THE FUTURE DUE TO NEW VULNERABILITIES OR POWERFUL QUANTUM COMPUTERS, LEADING TO POTENTIAL COMPROMISE OF STORED, INTERCEPTED DATA.

Man-in-the-middle attacks

- Man-in-the-Middle Attacks Intercept and Proxy: This special type of interception involves an attacker proxying data between sender and recipient to conceal the interception.
- Proxying Masks the Attack: The attacker intercepts requests, forwards them to the intended destination (modified or unmodified), and relays the responses back, making the interception difficult to detect.
- Legitimate Responses Deceive the Sender: The sender receives expected responses, believing they are communicating directly with the legitimate server.
- Attackers Can Capture Correct Credentials: By proxying, attackers can steal credentials and even prompt for the correct password if the user initially enters an incorrect one.



Data Theft

- Many cyberattacks involve stealing the victim’s data. An attacker may want to steal data belonging to individuals, businesses, or a government agency for one or more of many possible reasons.
- People, businesses, nonprofits, and governments are all vulnerable to data theft.

Personal data theft

- Criminals often try to steal people's data in the hope of finding items that they can monetize, including:
  - Data that can be used for **identity theft** or sold to identity thieves
  - Compromising photos or health-related data that may be sellable or used as part of extortion schemes
  - Information that is stolen and then erased from the user's machine can be ransomed to the user
  - Password lists that can be used for breaching other systems
  - Confidential information about work-related matters that may be used to make illegal stock trades based on insider information
  - Information about upcoming travel plans that may be used to plan robberies of the victim's home

Business data theft

- Criminals can use data stolen from businesses for several bad purposes
- **Making stock trades**: Criminals seek to steal data to have advanced knowledge of how a particular business's current and yet unreported quarter is going. They then use that insider information to illegally trade stocks or options, thereby potentially making a significant profit.
- **Selling data to unscrupulous competitors**: Criminals who steal sales pipeline information, documents containing details of future products, or other sensitive information can sell that data to unscrupulous competitors or to unscrupulous employees working at competitors whose management may never find out how such employees suddenly improved their performance.

Business data theft

- **Leaking data to the media**: Sensitive data can embarrass the victim and cause its stock to decline (perhaps after selling short some shares).
- **Recruiting employees**: By recruiting employees or selling the information to other firms looking to hire employees with similar skills or with knowledge of competition' systems, criminals who steal emails and discover communication between employees that indicates that one or more employees are unhappy in their current positions can sell that information to parties looking to hire.

Business data theft

- **Stealing and using intellectual property**: Parties that steal the source code for computer software may be able to avoid paying licensing fees to the software's rightful owner. Parties that steal design documents created by others after extensive research and development can easily save millions of dollars — and, sometimes, even billions of dollars — in research and development costs.