

# Topic: Introduction to Cyber Attacks

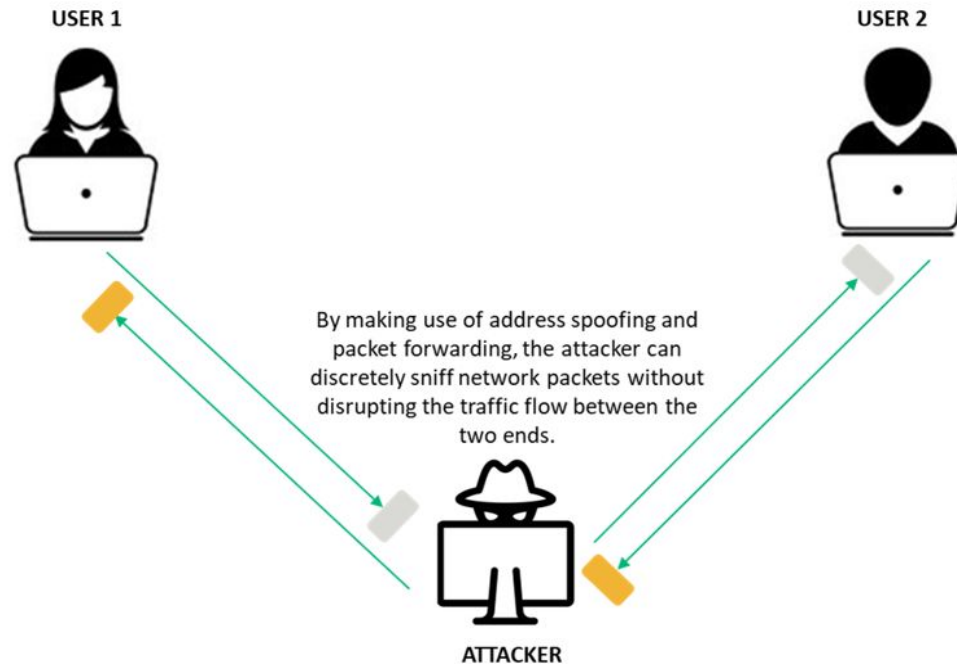
**Presented By:**

Rakib Hossen  
Assistant Professor  
Dept. of Cyber Security Engineering (CySE), UFTB

# What is “Attack” in Cyber Security

**Attacks = Motive (Goal) + Method + Vulnerability**

An **attack** is an **information security threat** that involves an attempt to obtain, alter, destroy, remove, implant or reveal information without **authorized access or permission**.

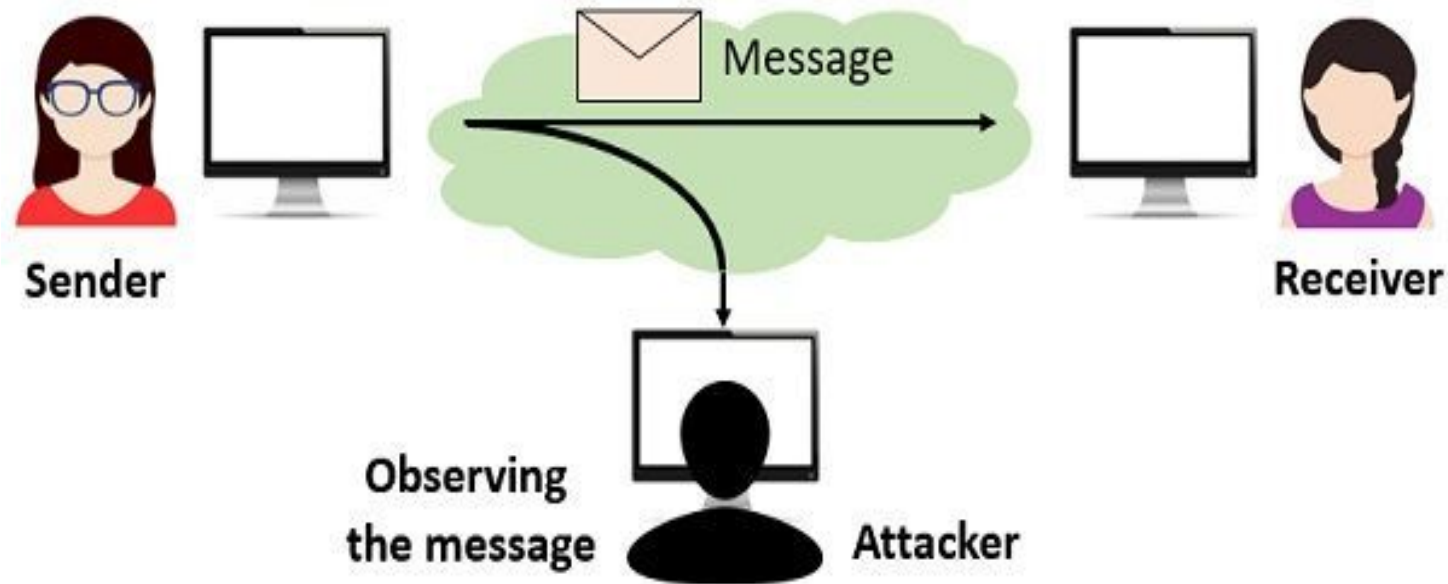


# Classification of Attack

<b>Passive Attacks</b>	<ul style="list-style-type: none"><li>• Passive attacks do not tamper with the data and involve intercepting and <b>monitoring network traffic</b> and data flow on the target network</li><li>• Examples include sniffing and eavesdropping</li></ul>
<b>Active Attacks</b>	<ul style="list-style-type: none"><li>• Active attacks tamper with the data in transit or <b>disrupt the communication</b> or services between the systems to bypass or break into secured systems</li><li>• Examples include DoS, Man-in-the-Middle, session hijacking, and SQL injection</li></ul>
<b>Close-in Attacks</b>	<ul style="list-style-type: none"><li>• Close-in attacks are performed when the attacker is in close physical proximity with the target system or network in order to gather, modify, or <b>disrupt access</b> to information</li><li>• Examples include social engineering such as eavesdropping, shoulder surfing, and dumpster diving</li></ul>
<b>Insider Attacks</b>	<ul style="list-style-type: none"><li>• Insider attacks involve using privileged access to <b>violate rules</b> or intentionally cause a threat to the organization's information or information systems</li><li>• Examples include theft of physical devices and planting keyloggers, backdoors, and malware</li></ul>
<b>Distribution Attacks</b>	<ul style="list-style-type: none"><li>• Distribution attacks occur when attackers <b>tamper with hardware</b> or <b>software</b> prior to installation</li><li>• Attackers tamper with the hardware or software at its source or in transit</li></ul>

# Passive Attack

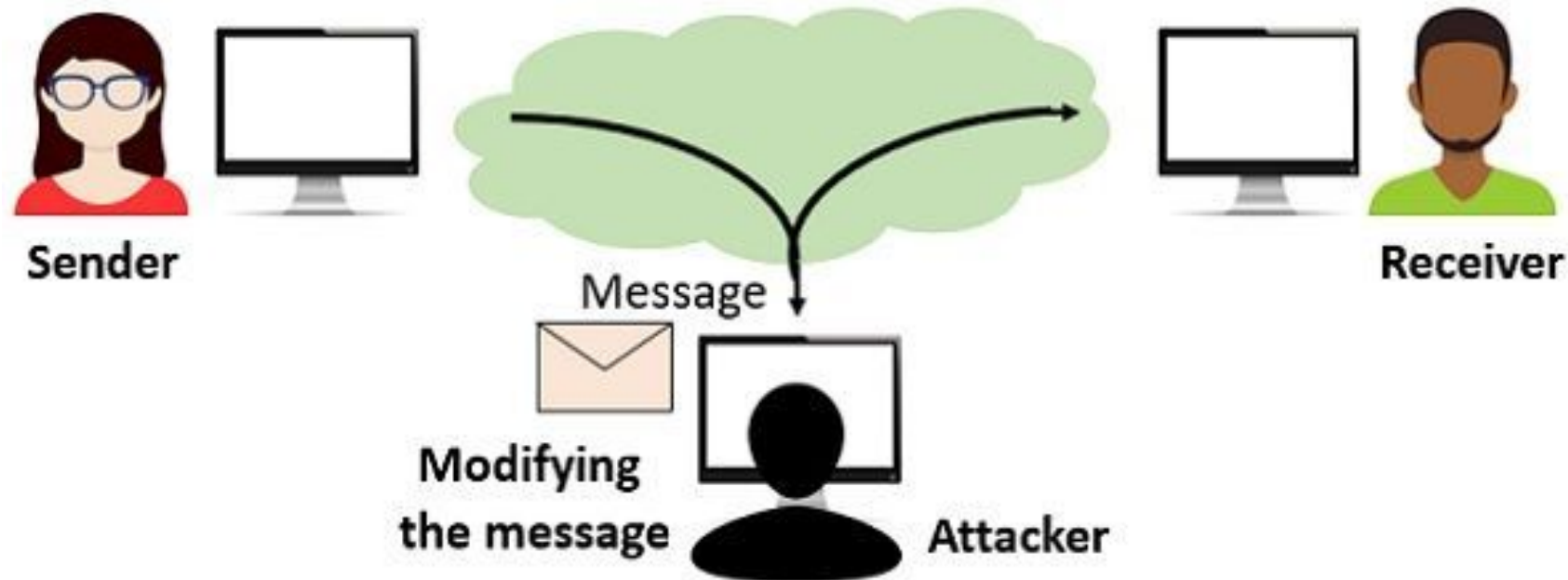
In passive attacks, the attacker does not alter the information but observes and monitors it, copies it, and then uses it to interfere in the network traffics and attack targeted machines. Intruding and monitoring of information is the main motive behind a Passive attack.



**Passive Attack**

# Active Attack

An Active attack attempts to alter system resources or affect their operations. Active attacks involve some modification of the data stream or the creation of false statements.

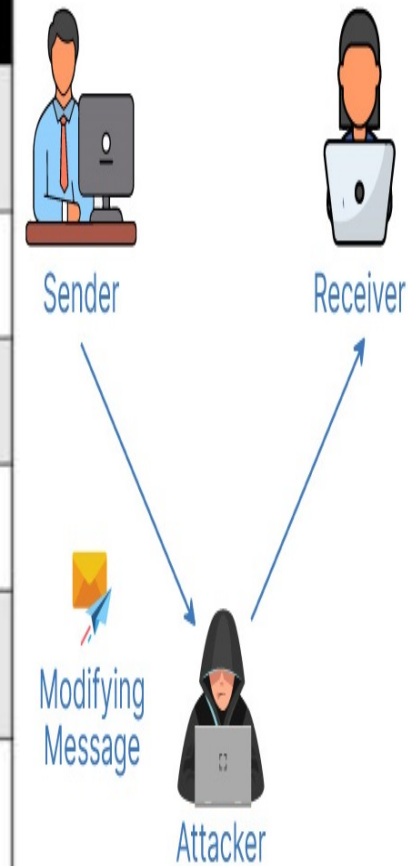


## Active Attack

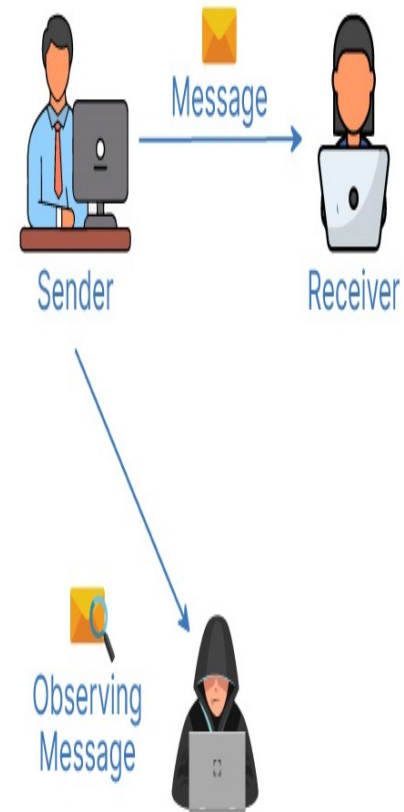


# Active Attack vs Passive Attack

No	Active Attack	Passive Attack
1	Attacker needs to have control media or network.	Attacker observe the communication in media or network.
2	It can be easily detected.	It cannot be easily detected.
3	It affects the system.	It does not affect the system.
4	It involves modification in data.	It involves in monitoring in data.
5	It does not check for loopholes or vulnerabilities.	It scans the ports and network in search for loopholes and vulnerabilities.
6	It is difficult to prevent network from active attack.	Passive attack can be prevented.
7	Types of active attack: Masquerade, replay, denial of service, modification of message.	Types of passive attack: release of message content, Traffic analysis.



**ACTIVE ATTACK**



**PASSIVE ATTACK**

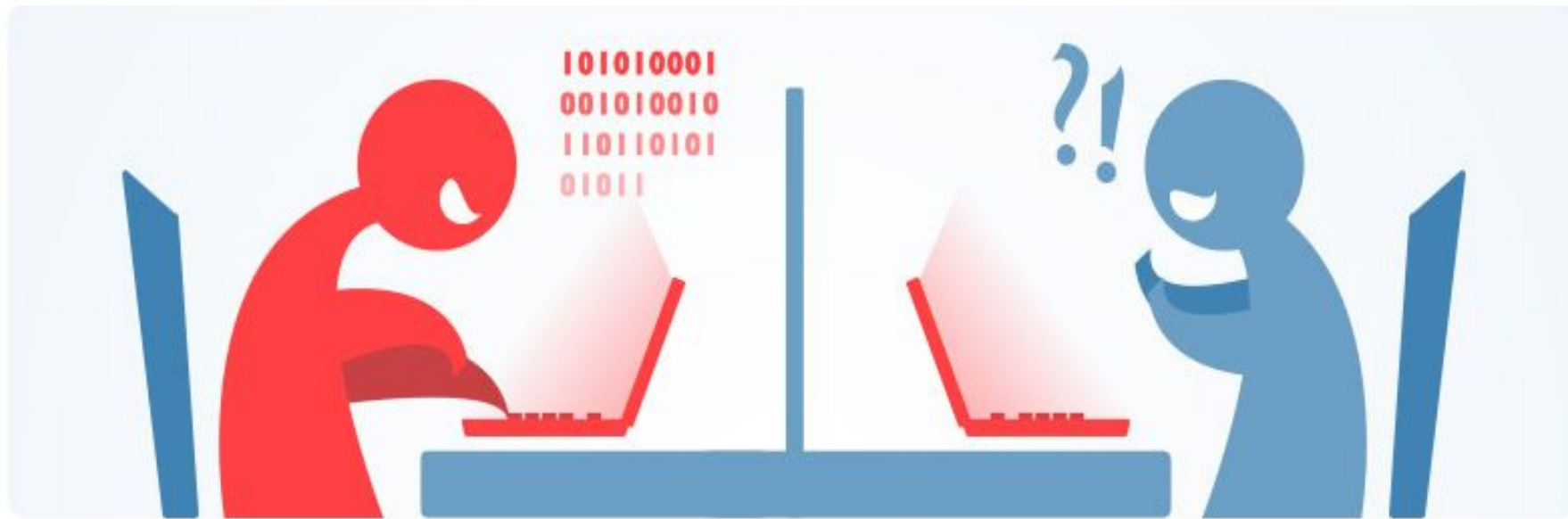
# Close-in Attack

A Close-in attack is a type of attack where the attacker is physically close to the target system. Attacker can take the advantages of being physically close to the target devices.



# Insider Attack

An insider attack is an attack from inside users ( a person with authorized system access.), who use their access credentials and knowledge of the network to attack the target machines.



## Malicious insiders

Intentionally use their access to sensitive data to harm the company

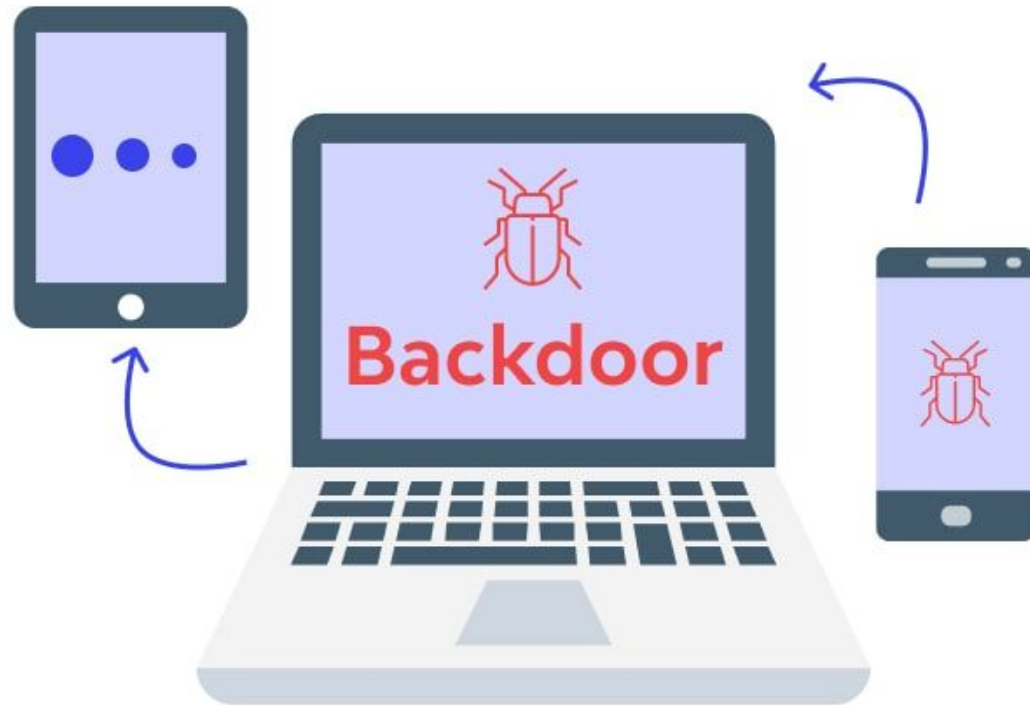
## Inadvertent insiders

Cause damage to the company unintentionally

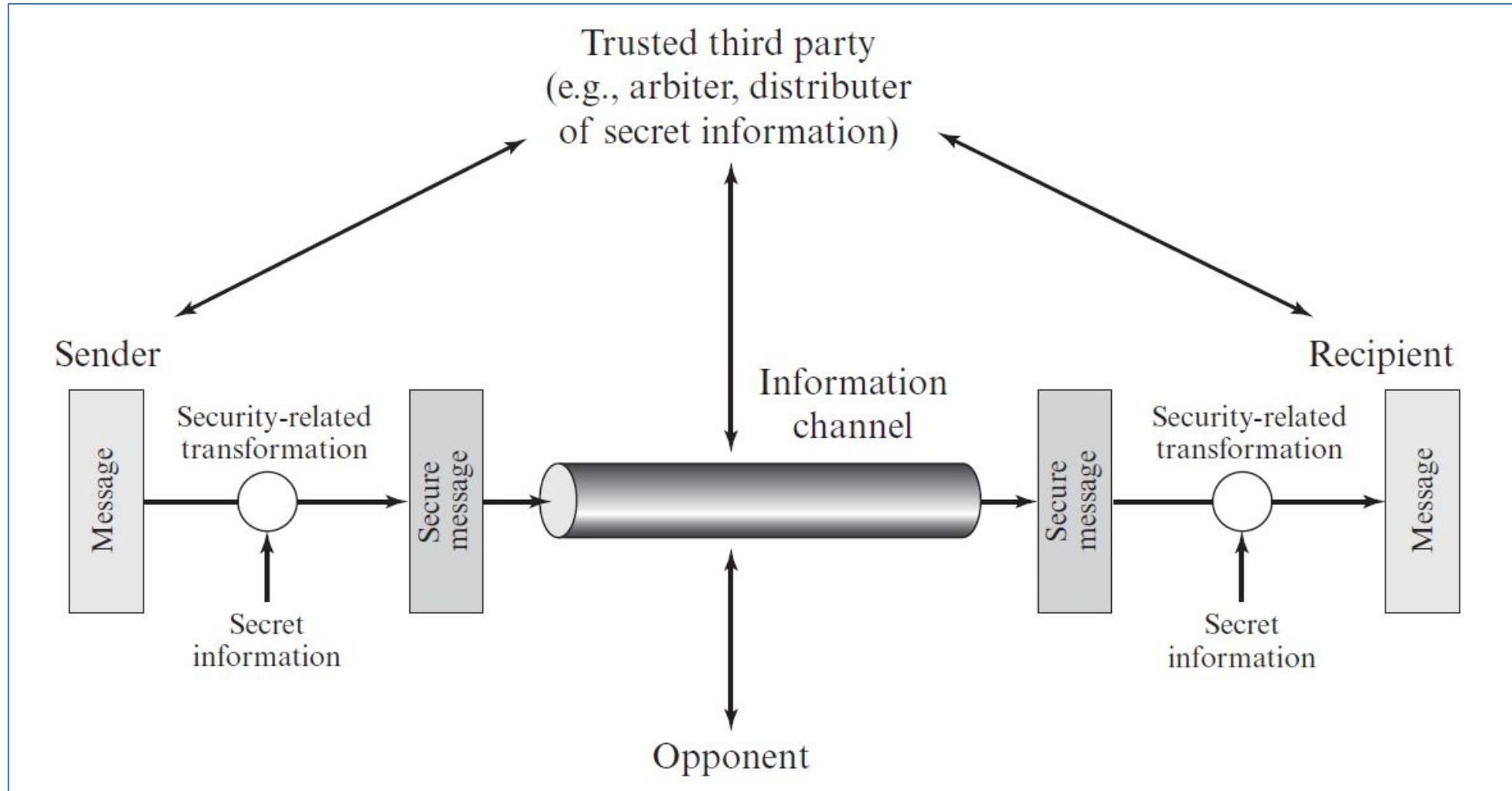


# Distribution Attack

Distribution attacks are the attacks using backdoors introduced to hardware or software systems at the time of manufacture. Once the hardware or software became functional, attackers can leverage the backdoor to attack the target devices.



# Model for Network Security



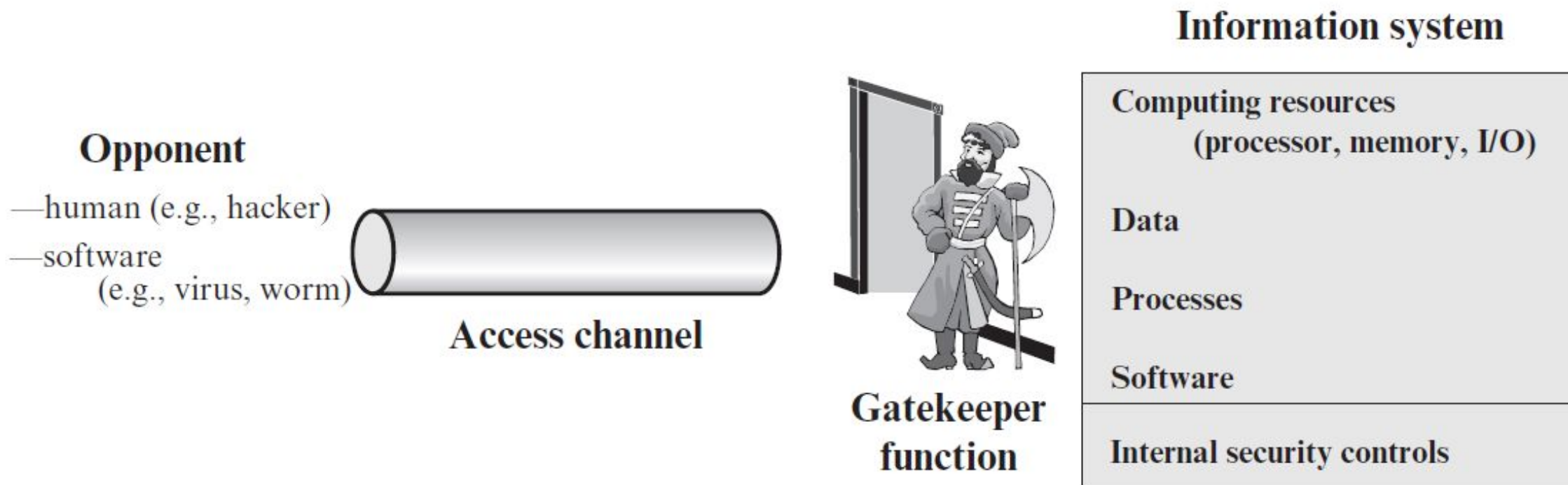
# Model for Network Security

- **Sender** wants to send a message to the **Recipient** in a confidential manner through the **Information Channel**.
- The Information Channel is considered insecure in nature.
- Therefore, if some third party (shown as **Opponent**) somehow gets the message, it will not be legible to the Opponent (that is, opponent must not be able to get any meaningful information from the message).
- To achieve the goal, Sender performs some security-related transformation of the message (called ***Encryption***) to convert the original message to a secure message. The Sender uses some secret information (called ***Key***) for the conversion.
- Afterwards, Sender sends the message to the Recipient via the insecurity channel.

# Model for Network Security

- Upon receipt, the Recipient performs another security-related transformation of the message (called ***Decryption***) to convert the secure message to the original message. The Recipient uses some secret information (called Key) for the conversion.
- The secured message is such that even though some opponent collects it during the transit, it will not be readable (that is, it would be impossible to get any useful meaning from the secure message).
- **Trusted Third Party** is some kind of service or company that both Sender and Recipient trusts for their secure communications.
- Most often, the Trusted Third Party sends a secret Key to both the Sender and Recipient via pre-established secure communication channels between itself and the Sender and Recipient.

# Model for Network Access Security

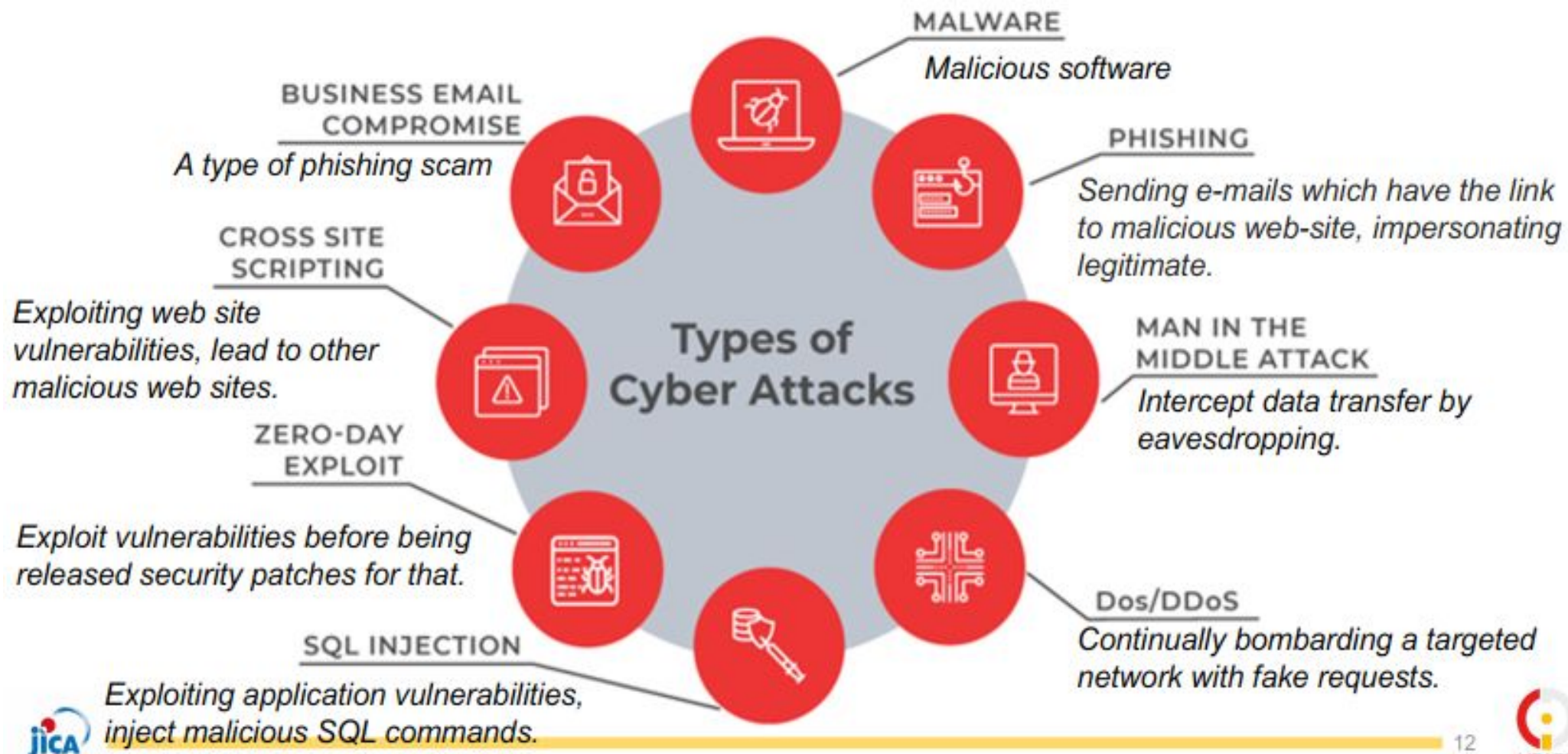


# Model for Network Access Security

- **Information System** is a very important component of any organization or company.
- There may be some legitimate users who may need to access the information system from outside the organization's network through the **Access Channel** (such as, MAN, WAN, or Internet).
- This provides opportunities to the **Opponents** (human opponents such as cybercriminals, and software opponents such as virus, worms) to try to access the information system through the Access Channel.
- **Gatekeeper Functions** are installed at the entry point of the organization's network.
- Such Gatekeeper Functions can be configured in network and security devices and software, such as Routers, Firewalls, Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and Gateways.



# Cyber Attacks



# Chance Cyber Attacks

## Chance for attackers

Better Chance for  
Attackers



AI



IoT



Big Data



Block Chain



Cloud Computing



AR & VR



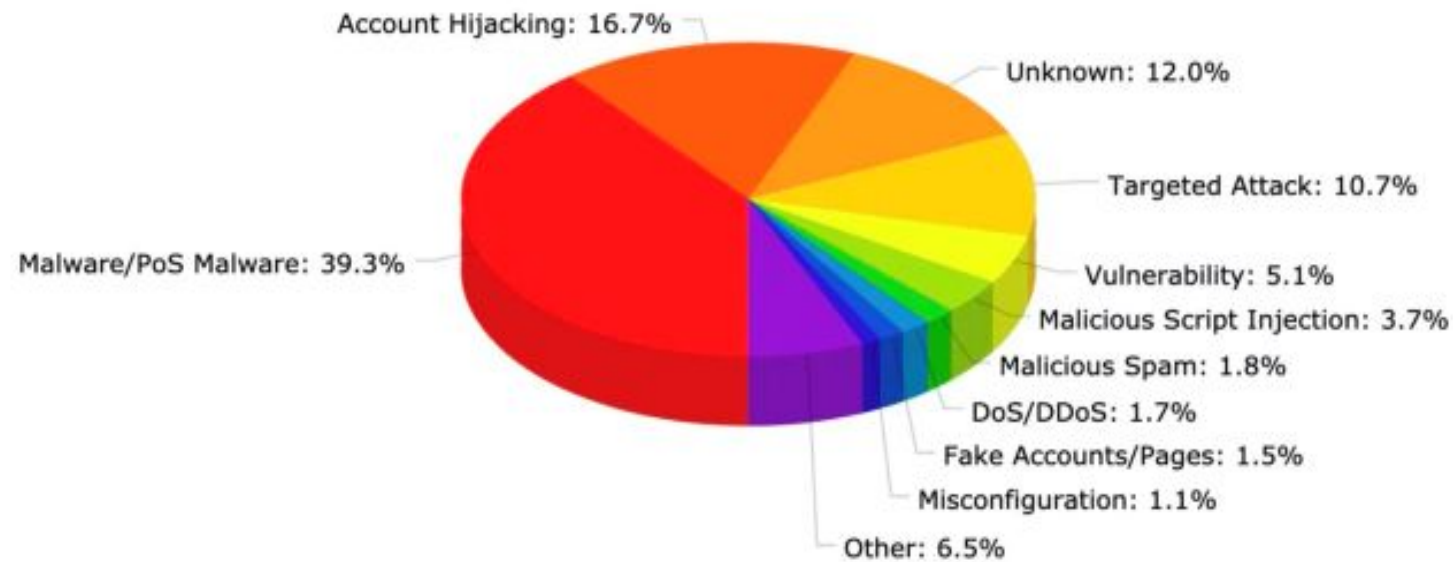
OSINT

# Trend of Cyber Attacks

## 2019 Cyber Attacks Statistics from HACKMAGGEDON

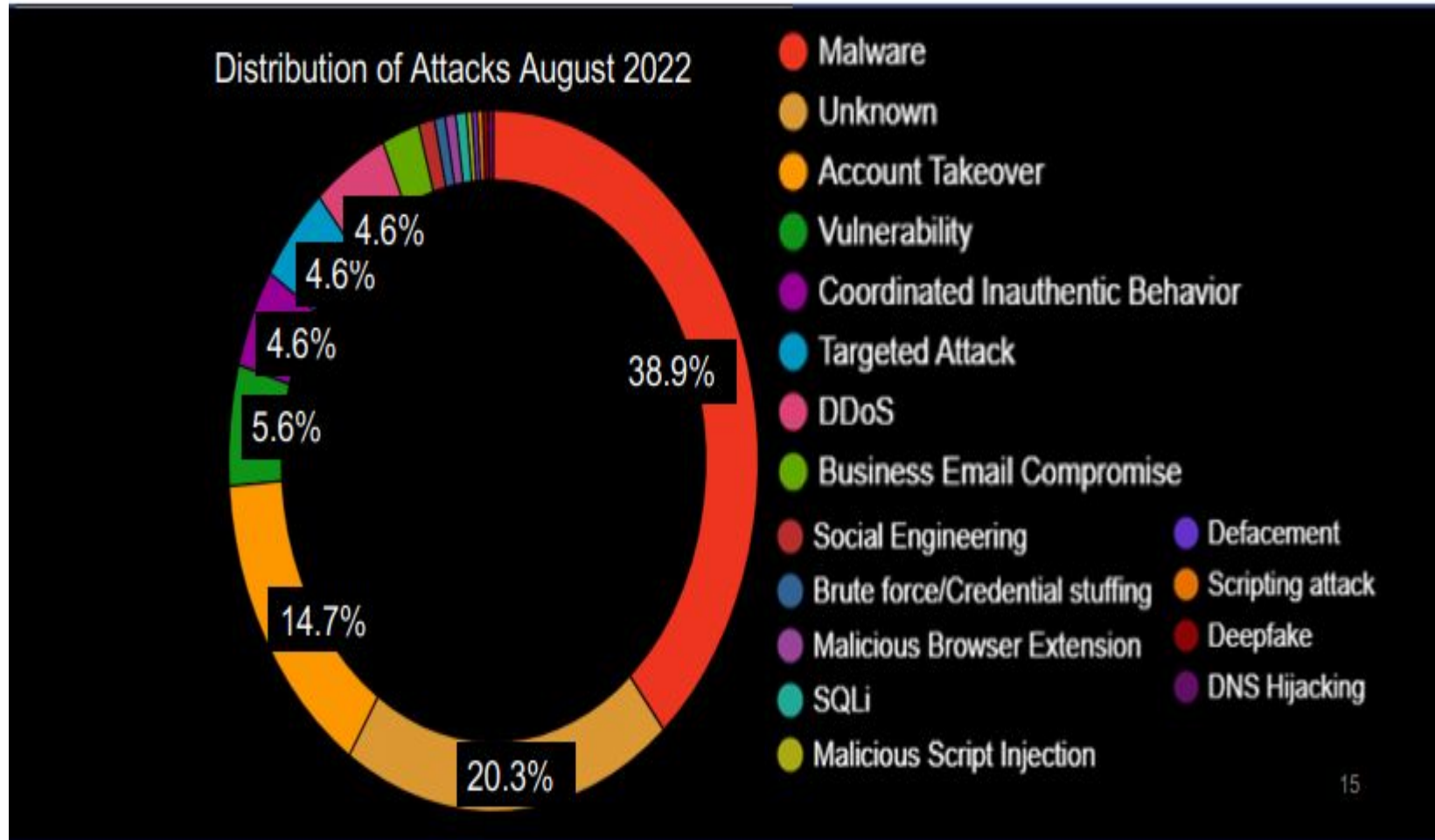
### Attack Distribution (Top 10 2019)

hackmageddon.com



# Trend of Cyber Attacks

## August 2022 Cyber Attacks Statistics from HACKMAGGEDON



# Impact of cyber attack

Cyber-attack or Leaked data can have impact on companies such as **Lost revenue**, **Reputational damage** and **Operational disruption**.

Show some Leaked Data as Demo



# Understanding Cyber-attack Situation

Insecam

Insecam

Most popular

Manufacturers

Countries

Places

Cities

Timezones

New online cameras

FAQ

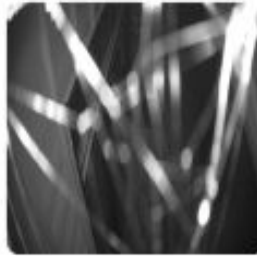
Contacts



## IP cameras: Japan



Watch Defeway camera in Japan, Kawasaki



Watch Defeway camera in Japan, Miyazaki



Watch Panasonic HD camera in Japan, Tokyo





# Understanding Cyber-attack Situation

<http://exploit-db.com>

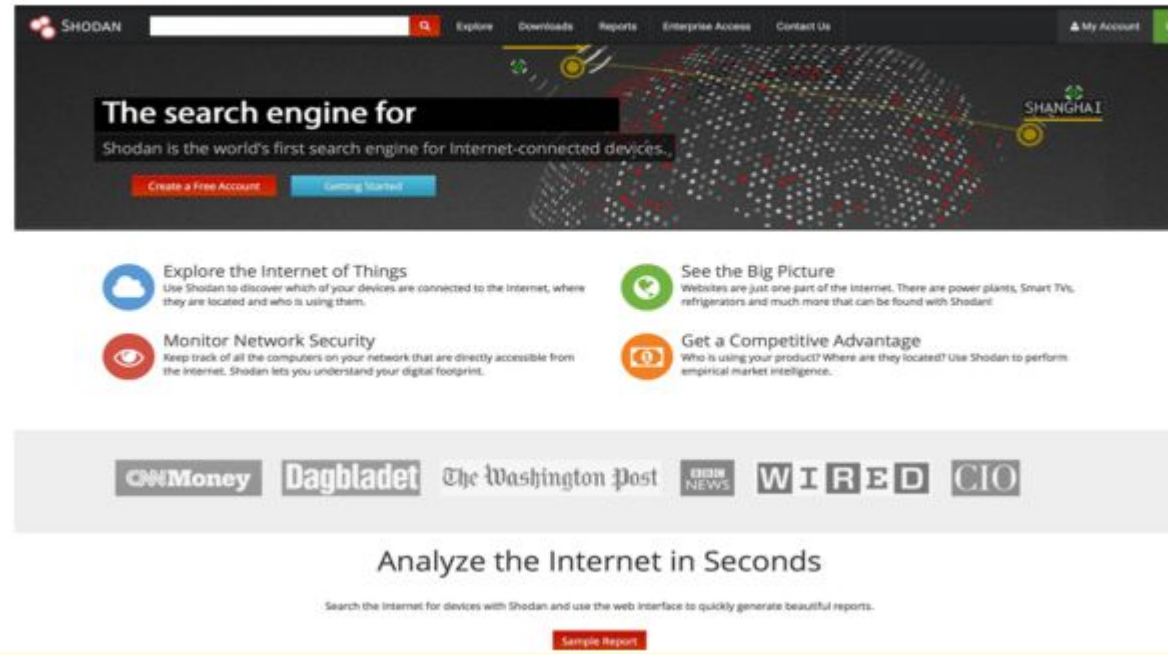


The screenshot shows the Exploit Database website. At the top, there's a navigation bar with links: Home, Exploits, Shellcode, Papers, Google Hacking Database, Submit, and Search. Below the navigation bar, the main heading is "Offensive Security Exploit Database Archive" with a count of "35484 Exploits Archived". A subtext reads: "The Exploit Database - ultimate archive of Exploits, Shellcode, and Security Papers. New to the site? Learn about the Exploit Database." Below this is a large banner for "The Exploit Database" with the text: "The Exploit Database (EDB) is a CVE compliant archive of exploits and vulnerable software. A great resource for penetration testers, vulnerability researchers, and security addicts alike. Our goal is to collect exploits from various sources and concentrate them in one, easy to navigate database." A button says "Download the Exploit Database Archive". To the right of the banner is a large "EXPLOIT DATABASE" logo with "CVE Compliant" and the CVE logo. Below the banner, the section "Remote Exploits" is highlighted. A subtext says: "This exploit category includes exploits for remote services or applications, including client side exploits." Below this is a table of exploits.

Date	D	A	V	Title	Platform	Author
2016-02-17	✓	-	✓	Inductive Automation Ignition 7.8.1 Remote Leakage Of Shared Buffers	multiple	LiquidWorm
2016-02-11	✓	-	✓	File Replication Pro <= 7.2.0 - Multiple Vulnerabilities	jsp	Vantage Point .
2016-02-10	✓	-	✓	D-Link DCS-930L Authenticated Remote Command Execution	hardware	metasploit

# Understanding Cyber-attack Situation

<http://shodan.io>



The screenshot displays the Shodan website homepage. At the top, there is a navigation bar with the Shodan logo, a search bar, and links for Explore, Downloads, Reports, Enterprise Access, and Contact Us. A user account link is also visible. The main banner features the text "The search engine for" followed by "Shodan is the world's first search engine for Internet-connected devices." Below this, there are two buttons: "Create a Free Account" and "Getting Started". The background of the banner shows a globe with numerous red and green dots representing connected devices. Below the banner, there are four feature sections, each with an icon and a title: "Explore the Internet of Things" (cloud icon), "See the Big Picture" (globe icon), "Monitor Network Security" (eye icon), and "Get a Competitive Advantage" (dollar sign icon). Each section includes a brief description of its capabilities. Below these sections, there is a row of logos for various media outlets: CNNMoney, Dagbladet, The Washington Post, BBC News, WIRED, and CIO. At the bottom, there is a section titled "Analyze the Internet in Seconds" with a subtext "Search the Internet for devices with Shodan and use the web interface to quickly generate beautiful reports." and a "Sample Report" button.

SHODAN

Explore Downloads Reports Enterprise Access Contact Us

My Account

The search engine for

Shodan is the world's first search engine for Internet-connected devices.

Create a Free Account Getting Started

Explore the Internet of Things  
Use Shodan to discover which of your devices are connected to the Internet, where they are located and who is using them.

See the Big Picture  
Websites are just one part of the Internet. There are power plants, Smart TVs, refrigerators and much more that can be found with Shodan!

Monitor Network Security  
Keep track of all the computers on your network that are directly accessible from the Internet. Shodan lets you understand your digital footprint.

Get a Competitive Advantage  
Who is using your product? Where are they located? Use Shodan to perform empirical market intelligence.

CNNMoney Dagbladet The Washington Post BBC NEWS WIRED CIO

Analyze the Internet in Seconds

Search the Internet for devices with Shodan and use the web interface to quickly generate beautiful reports.

Sample Report

# Understanding Cyber-attack Situation

## Cyber Attack Guide From Russian Hackers

- Advanced Hacking Guide with Metasploit
- Malware Development (RATS, botnets, Rootkits)
- Convert exe into PDF, XLS, DOC, JPG
- Exploit development guide
- Tech Tricks (Spoofing-SMS, email, call)
- Download any Free Apple Apps



# Understanding Cyber-attack Situation

## Cyber Attack Guide From Russian Hackers

- Credit Card Hacking
- Netbanking Hacking-bypass Virtual Keyboard
- Spreading guide to Infect 100K/Victims per day
- Advanced Email Hacking Tricks
- SET(Social Engineering Toolkit) module
- Links to other Russian hacking sites



# Types of Cyber Attacks

A cyber-attack is an exploitation of computer systems and networks.

It uses malicious code to alter computer code, logic or data and lead to cybercrimes, such as information and identity theft.

Due to the dependency on digital things, the illegal computer activity is growing and changing like any type of crime.

Cyber-attacks can be classified into the following categories:



**Classification of Cyber attacks**

# Web-based Attacks

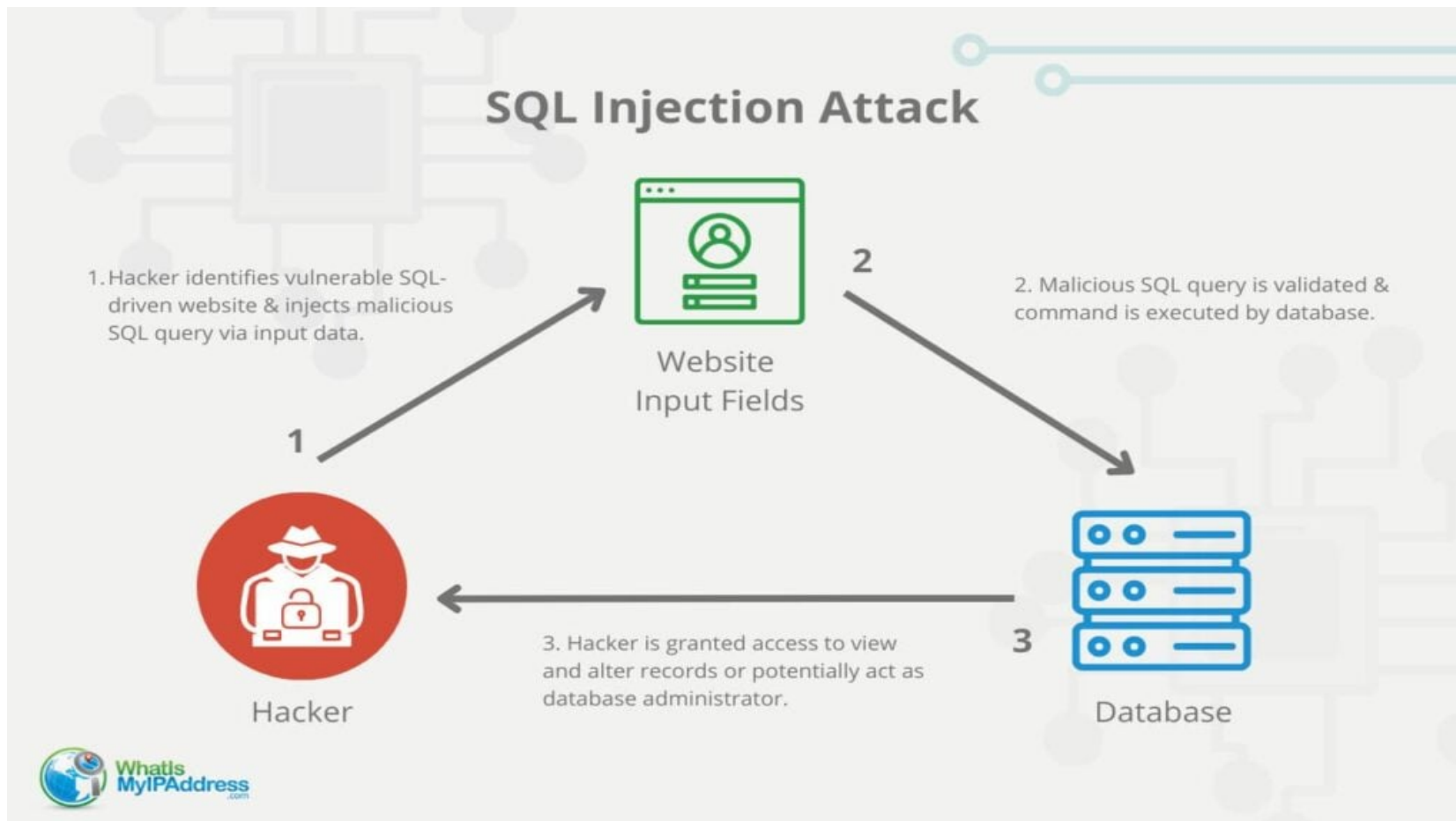
These are the attacks which occur on a website or web applications. Some of the important web-based attacks are as follows-

- ✓ **Injection attacks**
- ✓ **DNS Spoofing**
- ✓ **Session Hijacking**
- ✓ **Phishing**
- ✓ **Brute force**
- ✓ **Denial of Service**
- ✓ **Dictionary attacks**
- ✓ **URL Interpretation**
- ✓ **Zero-Day Exploit**
- ✓ **File Inclusion attacks**
- ✓ **Man in the middle attacks**
- ✓ **Cross-site scripting**
- ✓ **Distributed Denial of Service (DDoS) attacks.**
- ✓ **Password Attack**
- ✓ **Cryptojacking**
- ✓ **Identity-Based Attacks**

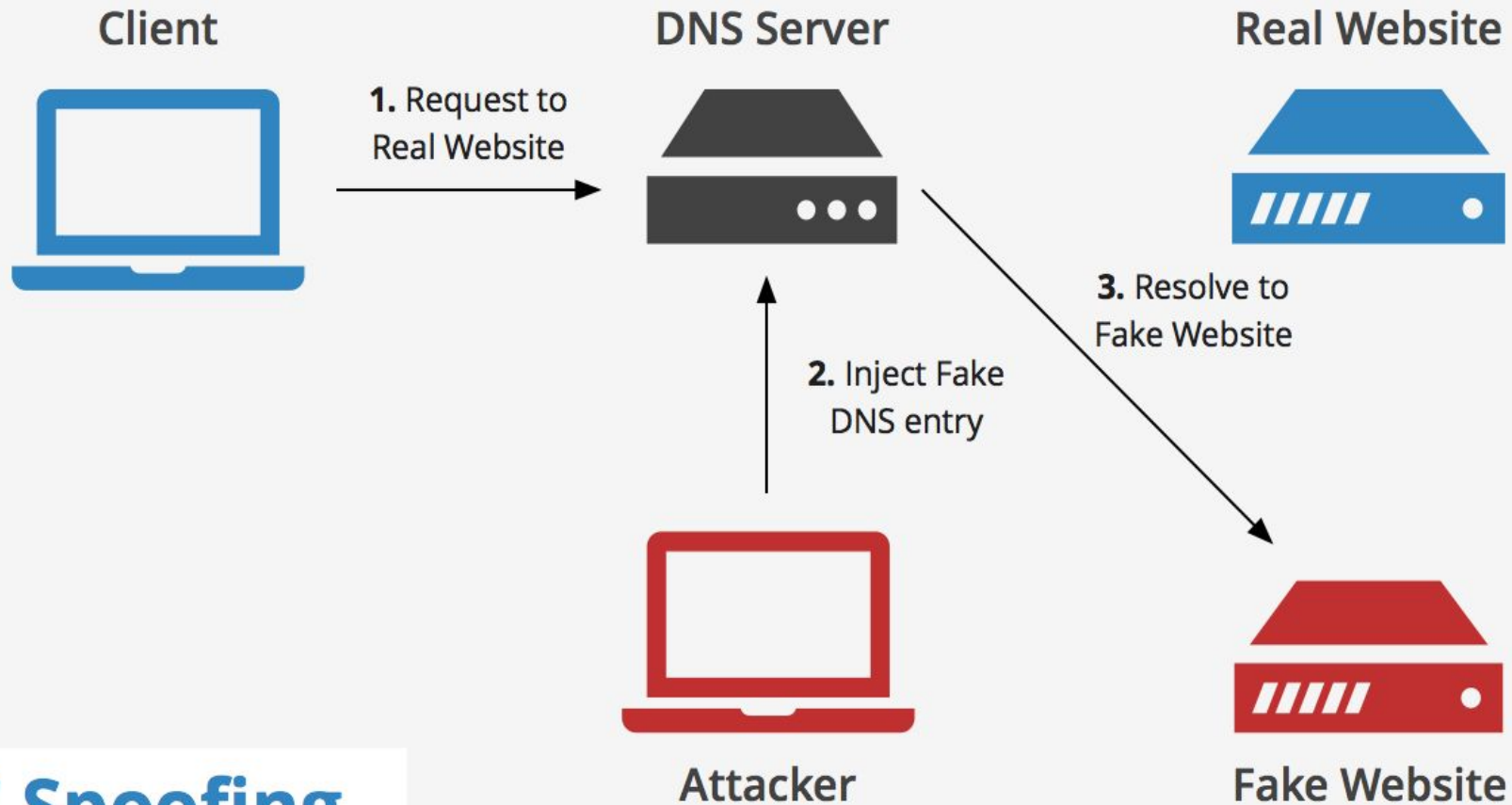


# Injection Attack

This type of attack allows an attacker to inject code into a program or query or inject malware onto a computer in order to execute remote commands that can read or modify a database or change data on a web site.



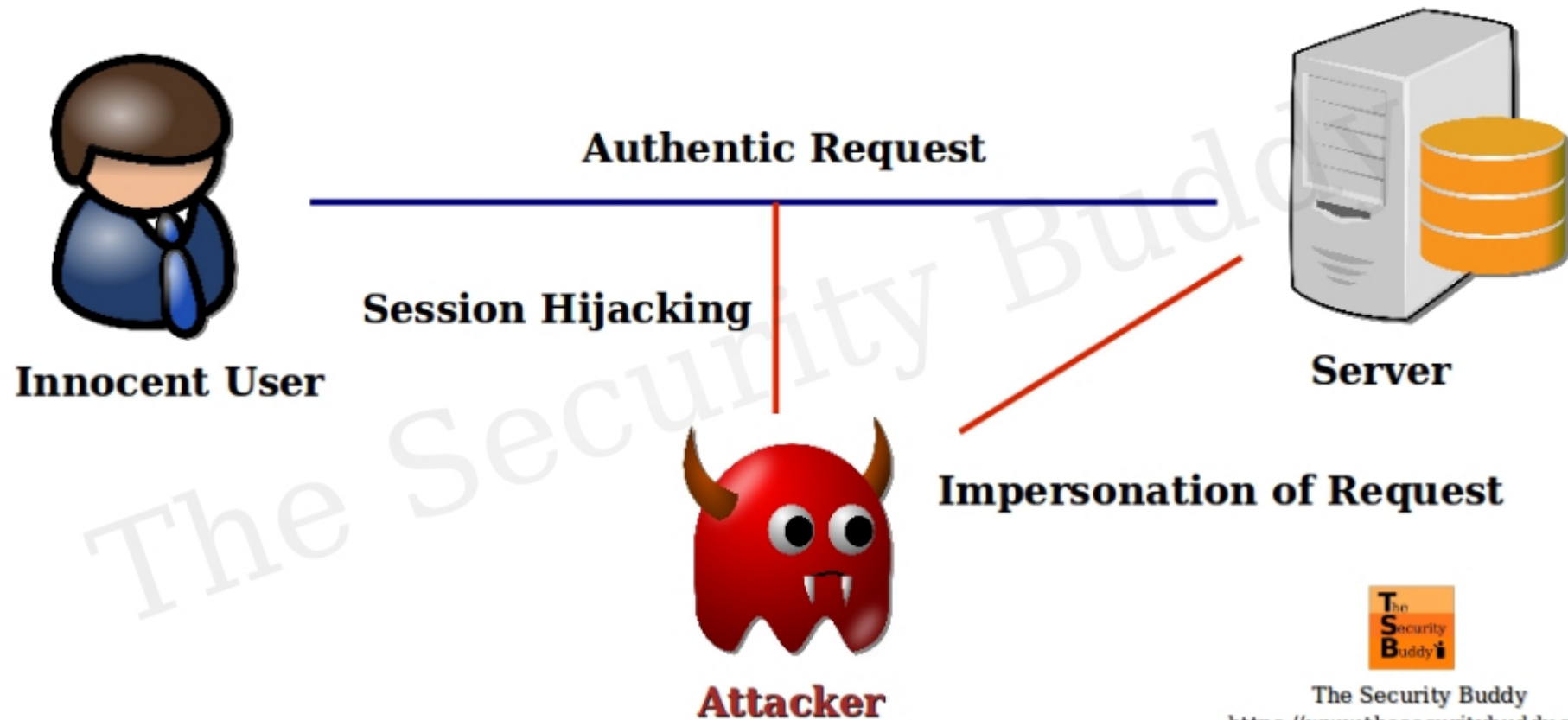
# DNS Spoofing



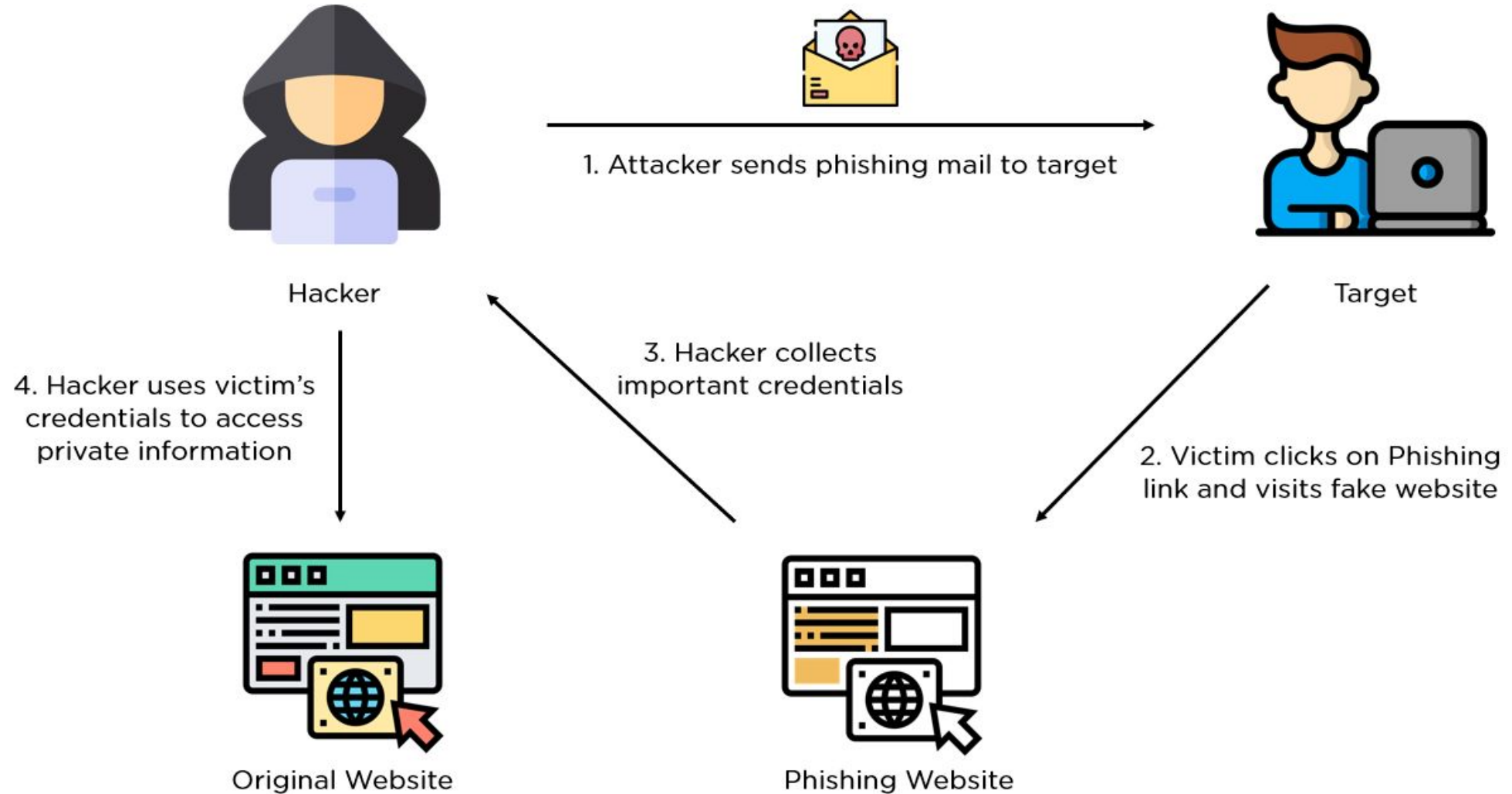
**DNS Spoofing**

# Session Hijacking

## Session Hijacking



# Phishing



# Brute Force



**Attacker**



**Guess List Of  
Username &  
Password  
Combination**

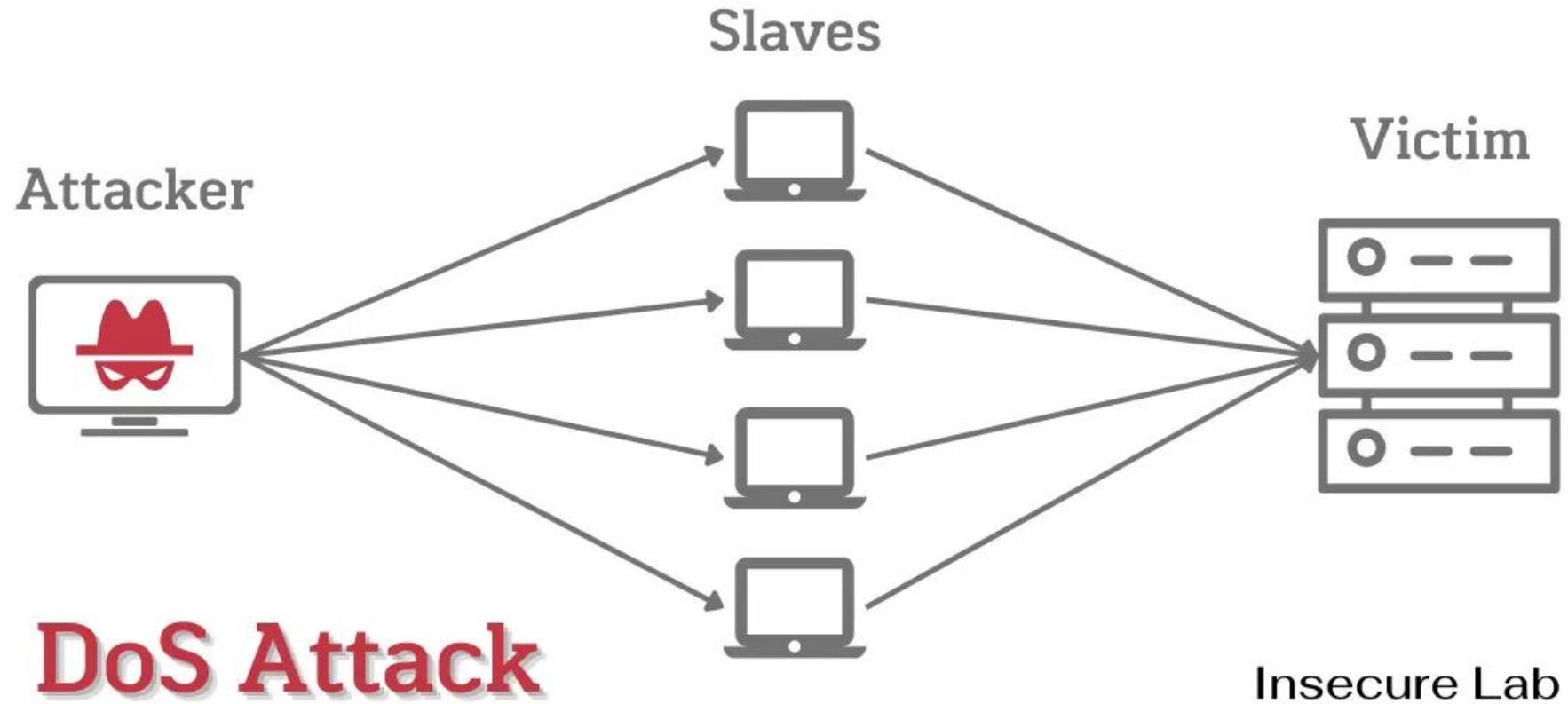


**Repeats Login  
Attempts Until  
One Is Successful**



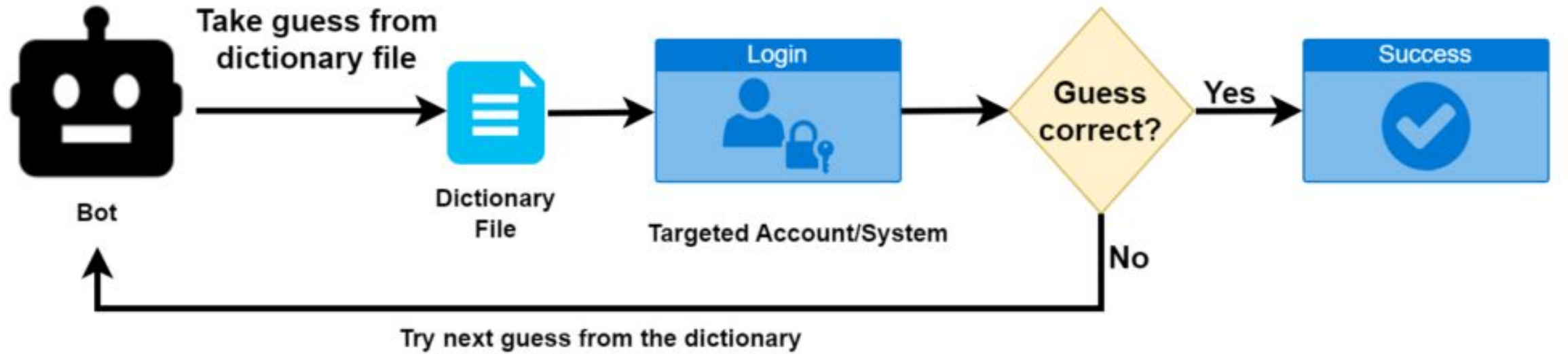
**Successful  
Credential Validation**

# Denial of Service (DoS) Attacks



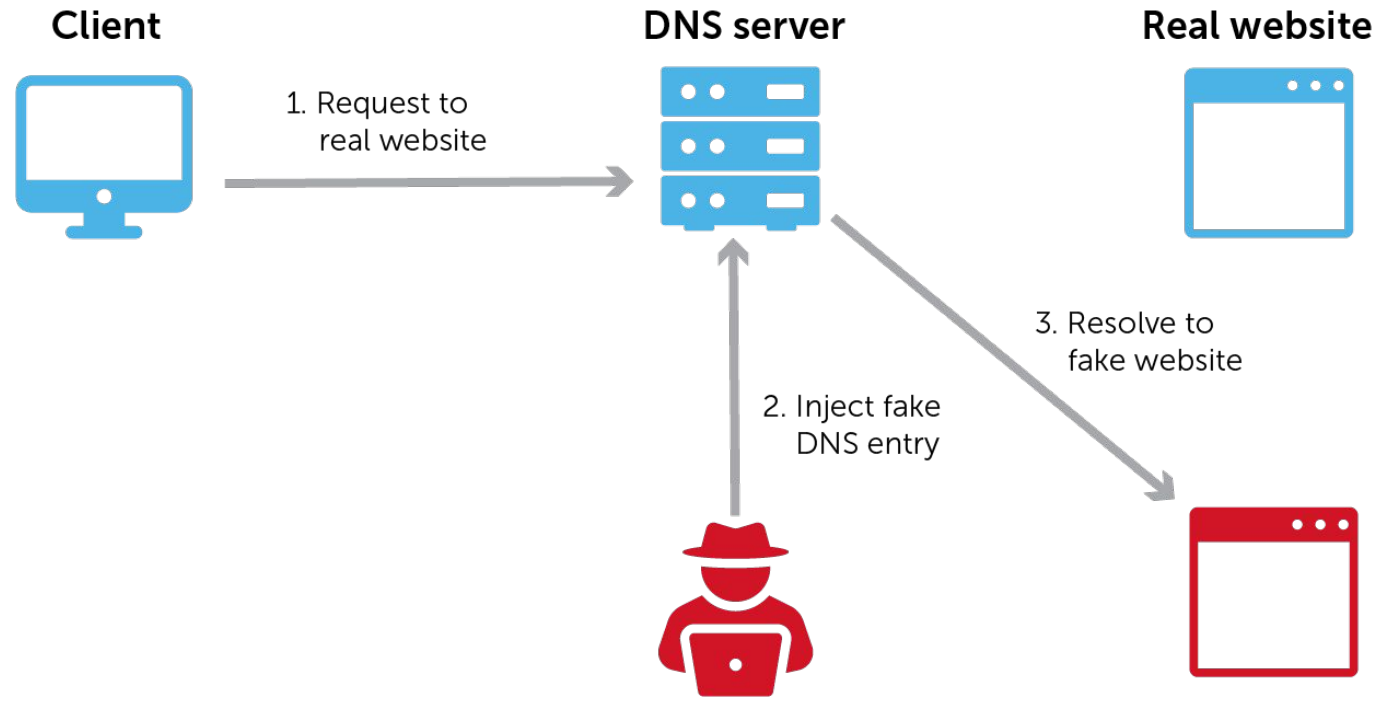


# Dictionary Attacks

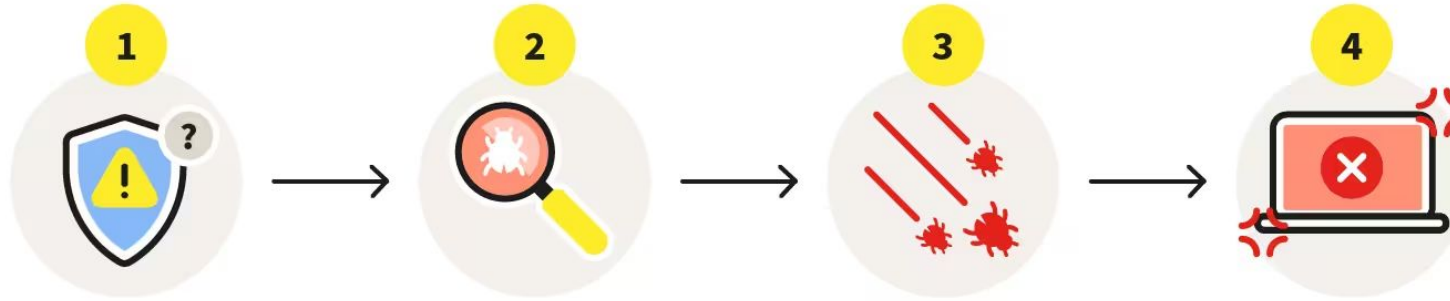


# URL Interpretation

## DNS poisoning



# Zero-Day Exploit



1

**A security flaw exists** but is unbeknown to developers, making it vulnerable to attacks.

2

**A hacker discovers** the vulnerability and exploits it by malware injection.

3

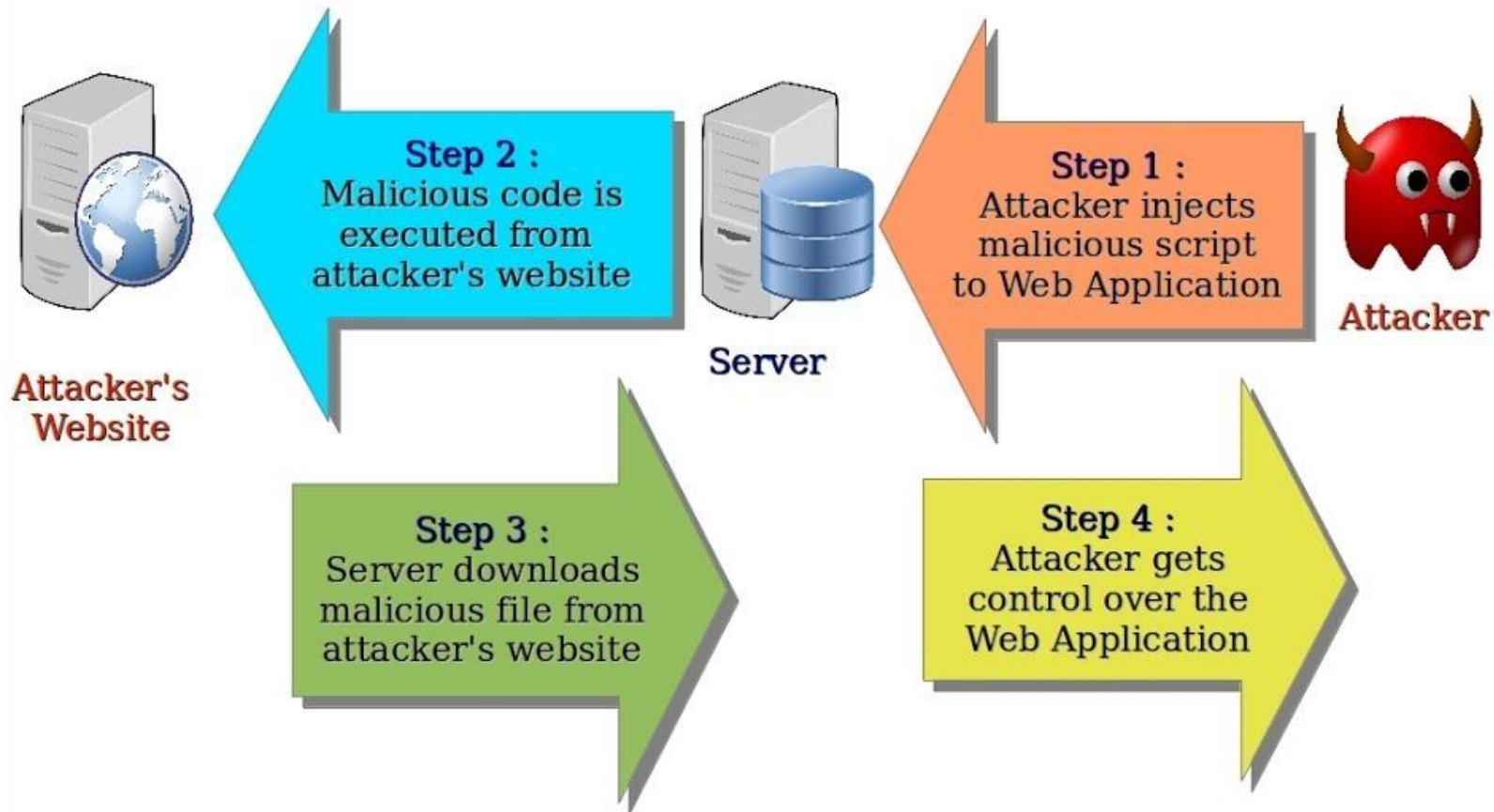
**A cyberattack ensues** from the malware, potentially resulting in data loss.

4

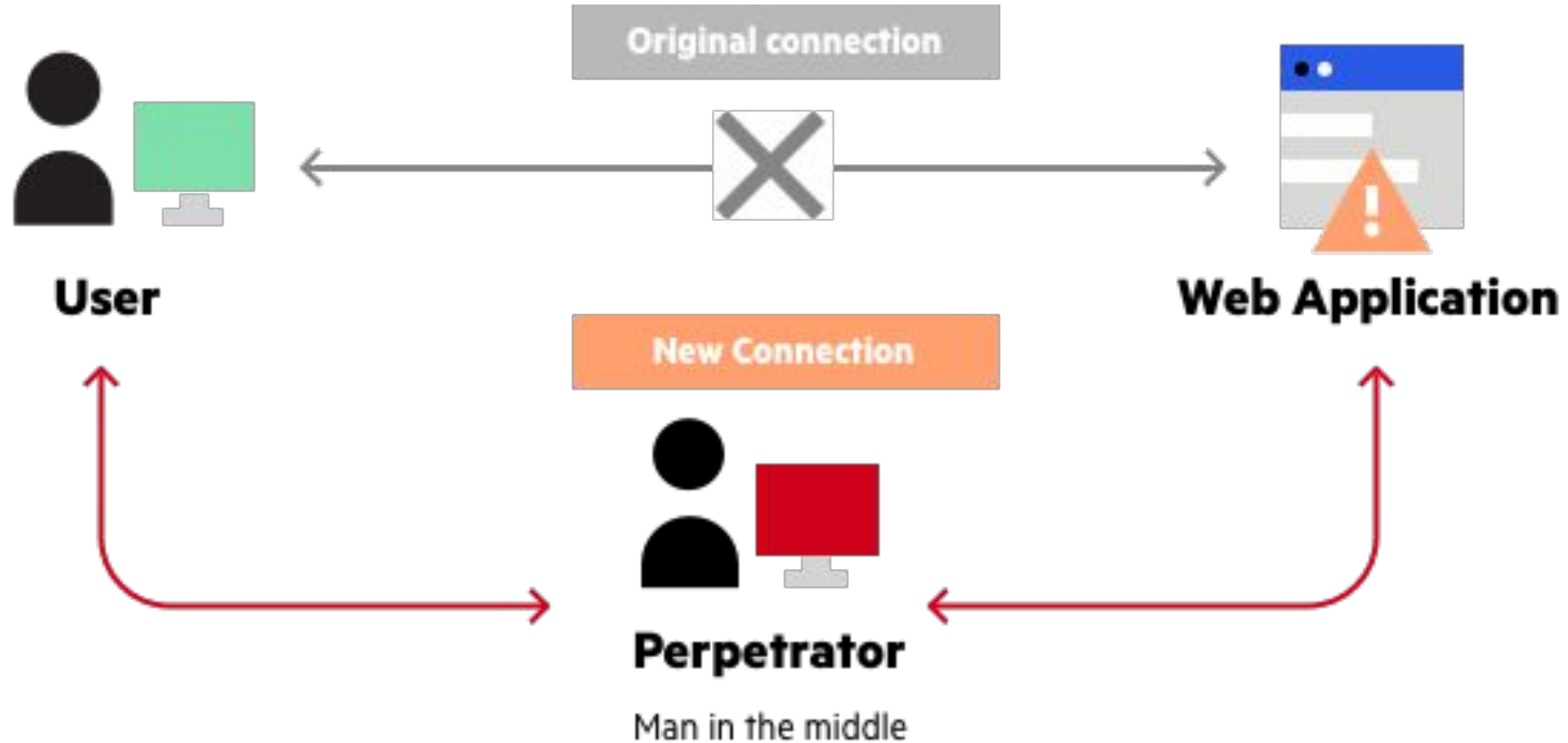
**Developers detect the attack** and have zero days to mitigate it.

# File Inclusion Attacks

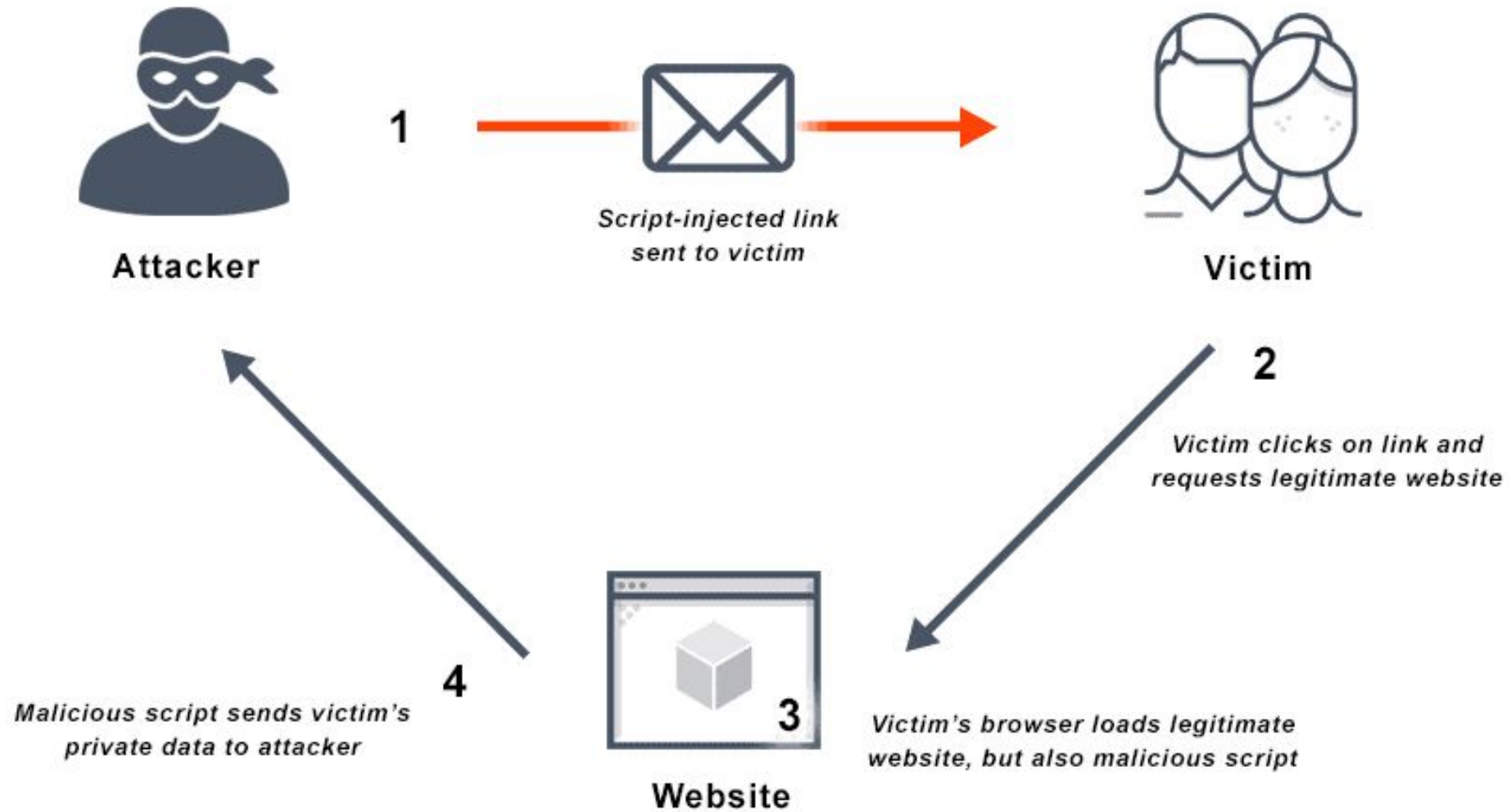
## File Inclusion Attack



# Man in the Middle Attacks

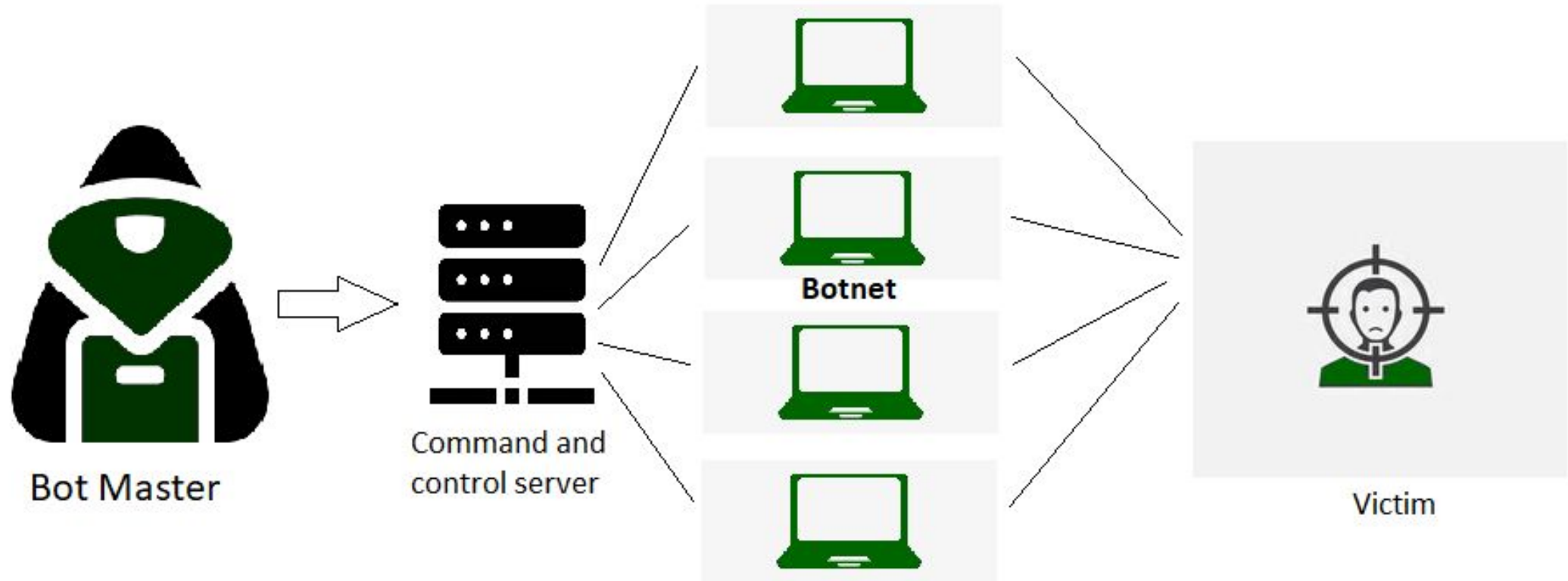


# Cross-Site Scripting

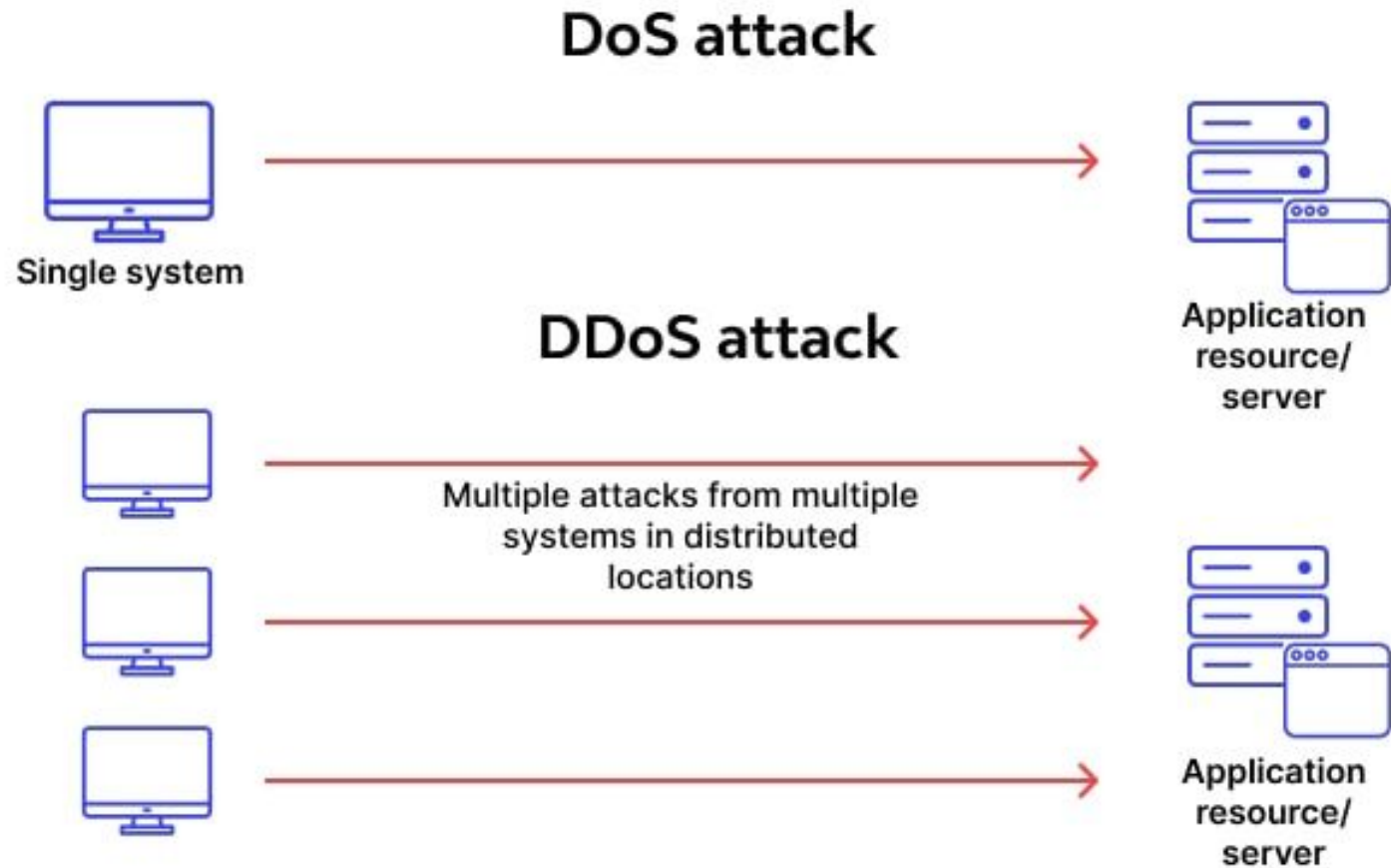




# Distributed Denial of Service (DDoS) Attacks

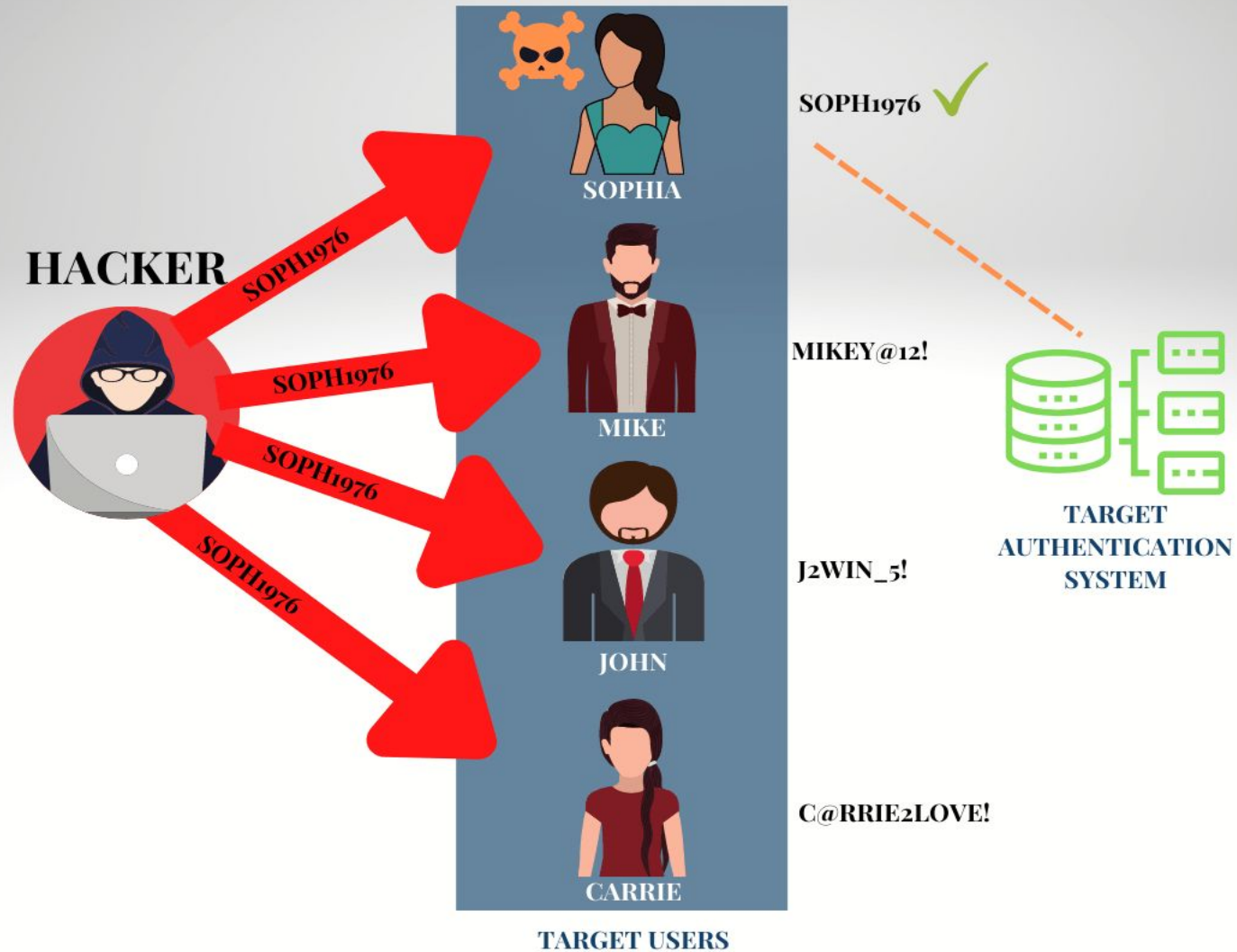


# DoS vs. DDoS Attacks

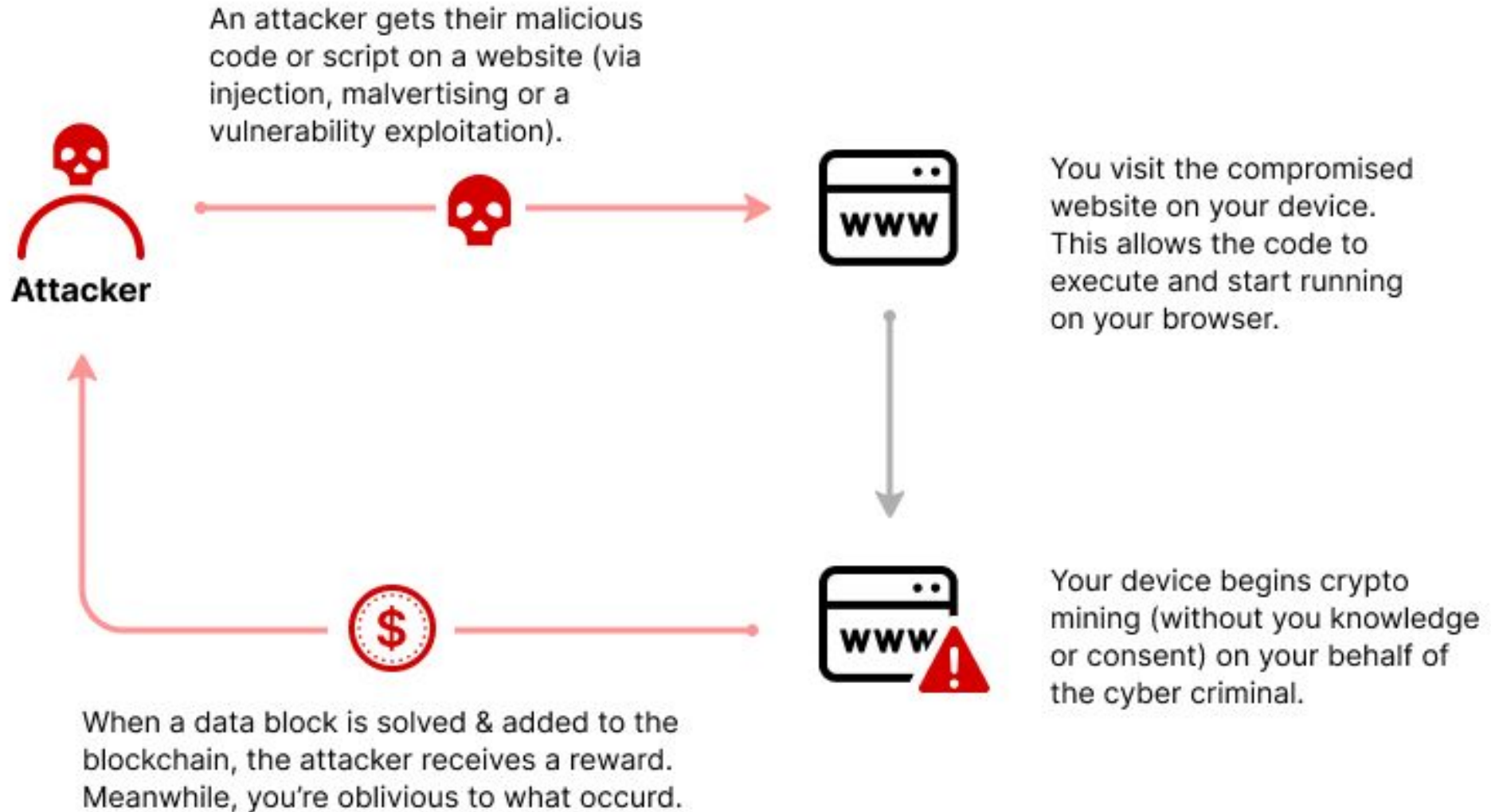


# Password Attack

## HOW A PASSWORD SPRAYING ATTACK WORKS



# Cryptojacking



# Identity-Based Attacks



Hacker gathers a list of commonly-used passwords



Hacker tries the same common password across multiple accounts



Once a login is successful, hacker harvests the sensitive data

# System-based Attacks

These are the attacks which are intended to compromise a computer or a computer network. Some of the important system-based attacks are as follows-

- ✓ **Virus**
- ✓ **Worm**
- ✓ **Trojan horse**
- ✓ **Backdoors**
- ✓ **Bots**



# What is Malware?

- ❖ "Malware" is a short term for "malicious software," and it refers to any software specifically designed to harm, exploit, or compromise computer systems, devices, or data without the user's consent.
- ❖ Malware includes various types of malicious programs such as viruses, worms, Trojans, spyware, adware, and ransomware, among others.
- ❖ Its primary intent is to infiltrate, disrupt, or steal information from a computer or network, and it can cause significant damage to both individuals and organizations.

# What is Malware? Cont...

The first malware, known as the "Creeper" virus, was created by Bob Thomas in the early 1970s. However, it wasn't as harmful as modern malware and was more of an experiment. Malicious software as we know it today evolved later.

Malware programmers develop and use malwares to

- Attack browsers and track websites visited
- Slow down systems and degrade system performance
- Cause hardware failure, rendering computers inoperable
- Steal personal information, including contacts
- Erase valuable information, resulting in substantial data loss
- Attack additional computer systems directly from a compromised system
- Spam inboxes with advertising emails

# What is Malware? Cont...

Example of a simple malware code

```
@echo off
```

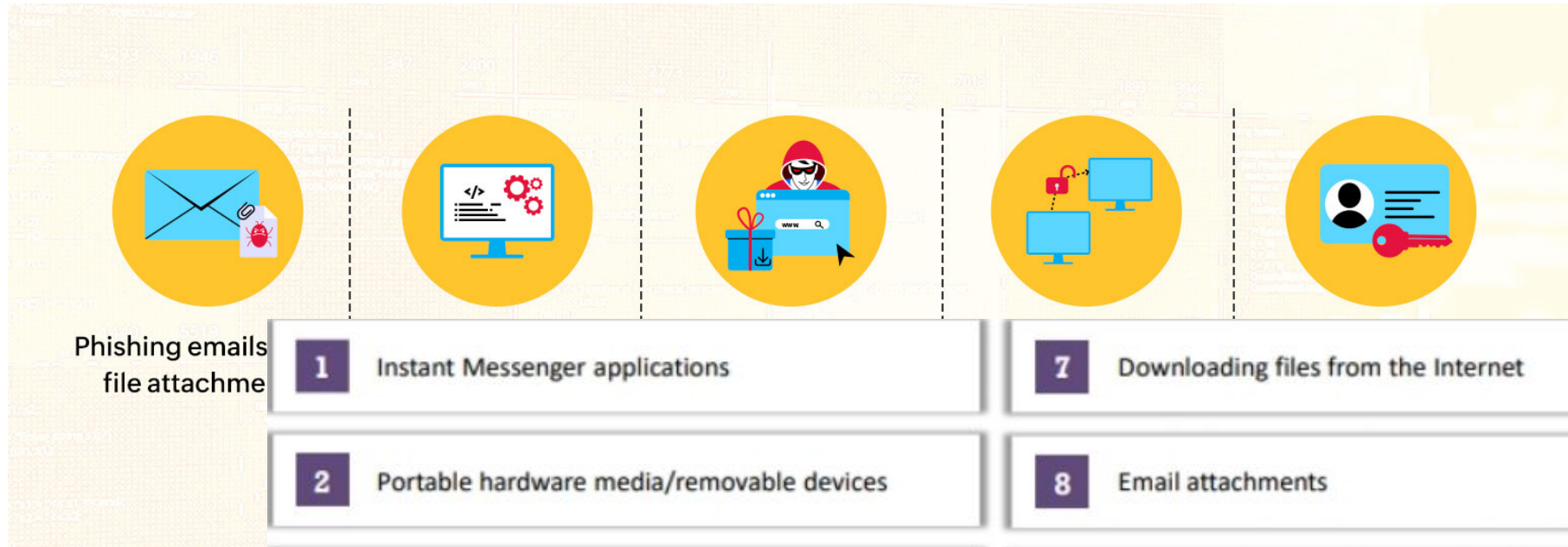
```
:A
```

```
start notepad
```

```
goto A
```

**Note:** This very simple batch program will continually open notepad until you get a restart the system.

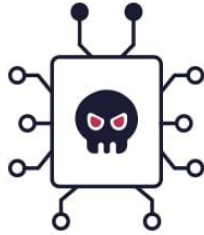
# Different ways malware can enter your network



# Different ways malware can enter your network

1	Instant Messenger applications	7	Downloading files from the Internet
2	Portable hardware media/removable devices	8	Email attachments
3	Browser and email software bugs	9	Network propagation
4	Insecure patch management	10	File sharing services (NetBIOS, FTP, SMB)
5	Rogue/decoy applications	11	Installation by other malware
6	Untrusted sites and freeware web applications/ software	12	Bluetooth and wireless networks

# Types of Malware



## **VIRUS**

Spreads between computers



## **WORM**

Spreads between computers in one company or location



## **TROJAN**

Sneaks malware onto your computer



## **SPYWARE**

Steals your data



## **ADWARE**

Spams you with ads



## **RANSOMWARE**

Encrypts files and blackmails you



## **FILELESS MALWARE**

Operates in your system's memory



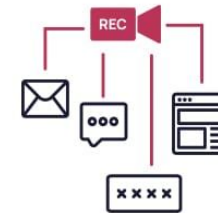
## **ROOTKIT**

Gives remote access to your device



## **BOTNET**

Turns your PC into a puppet



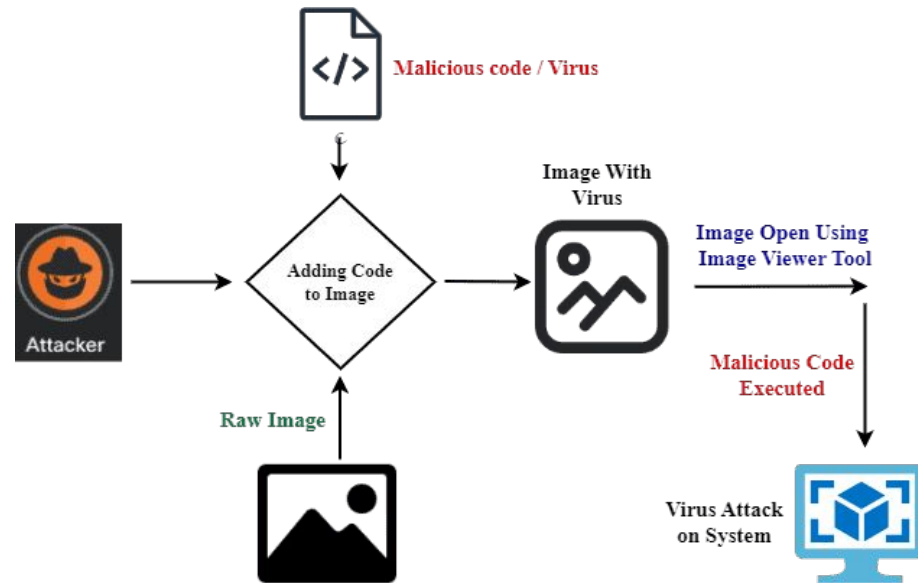
## **KEYLOGGER**

Records user activity



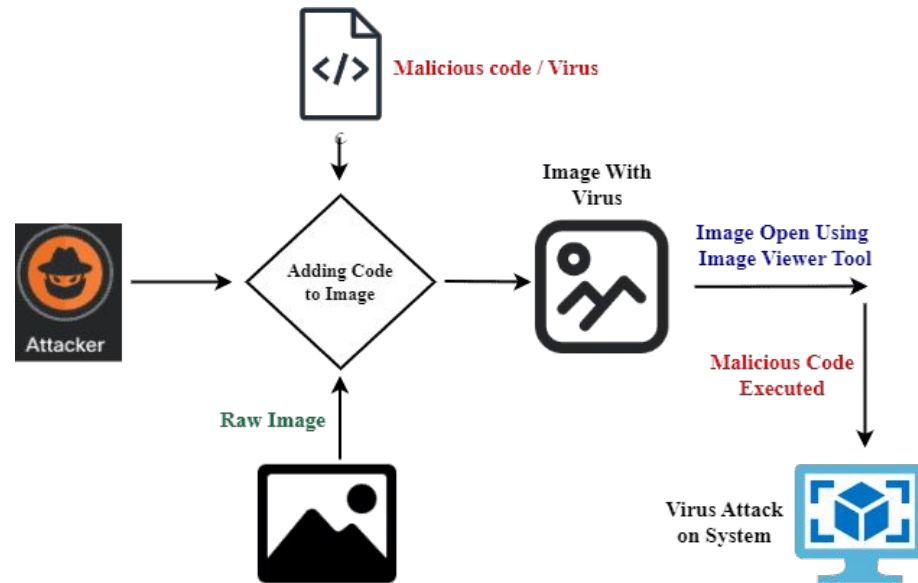
# Viruses

- A computer virus is a malicious program that infects files or the system areas of a computer and then makes copies of itself.
- Viruses are harmful and can corrupt data and files; however, some viruses are harmless, too.
- Computer viruses need a host to replicate. When you run or open an infected file or program, the virus attaches itself to other files, spreading its code and potentially causing harm.

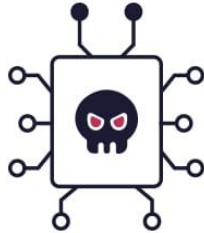


# Viruses

- A computer virus is a malicious program that infects files or the system areas of a computer and then makes copies of itself.
- Viruses are harmful and can corrupt data and files; however, some viruses are harmless, too.
- Computer viruses need a host to replicate. When you run or open an infected file or program, the virus attaches itself to other files, spreading its code and potentially causing harm.



# Types of Malware



## **VIRUS**

Spreads between computers



## **WORM**

Spreads between computers in one company or location



## **TROJAN**

Sneaks malware onto your computer



## **SPYWARE**

Steals your data



## **ADWARE**

Spams you with ads



## **RANSOMWARE**

Encrypts files and blackmails you



## **FILELESS MALWARE**

Operates in your system's memory



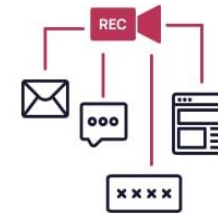
## **ROOTKIT**

Gives remote access to your device



## **BOTNET**

Turns your PC into a puppet



## **KEYLOGGER**

Records user activity

Thank You