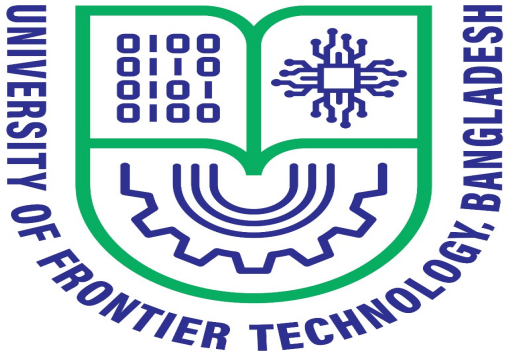


Topic: Introduction to Cyber Attacks

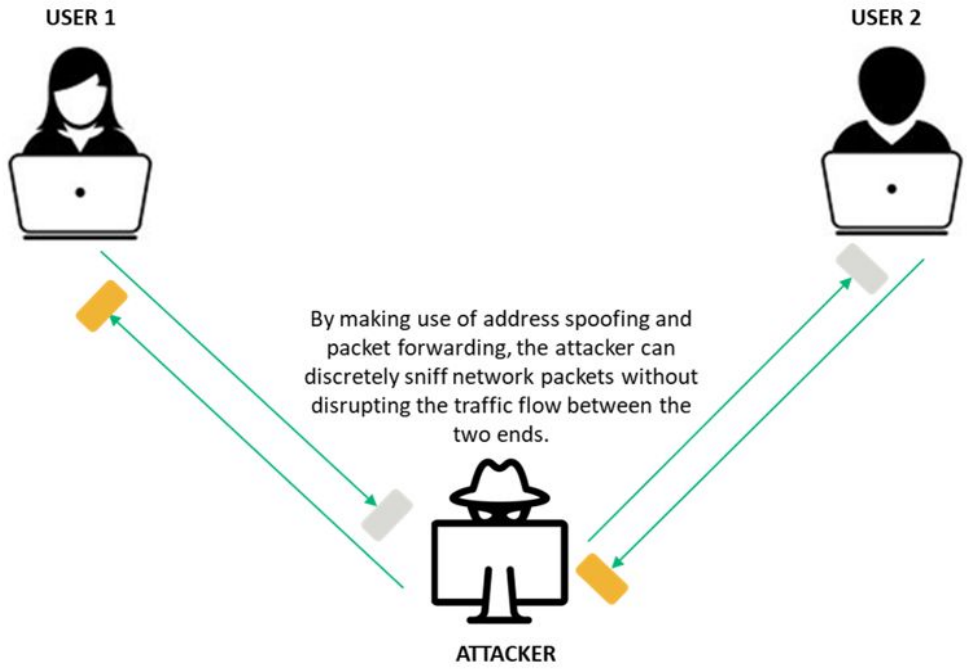
Presented By:

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.**

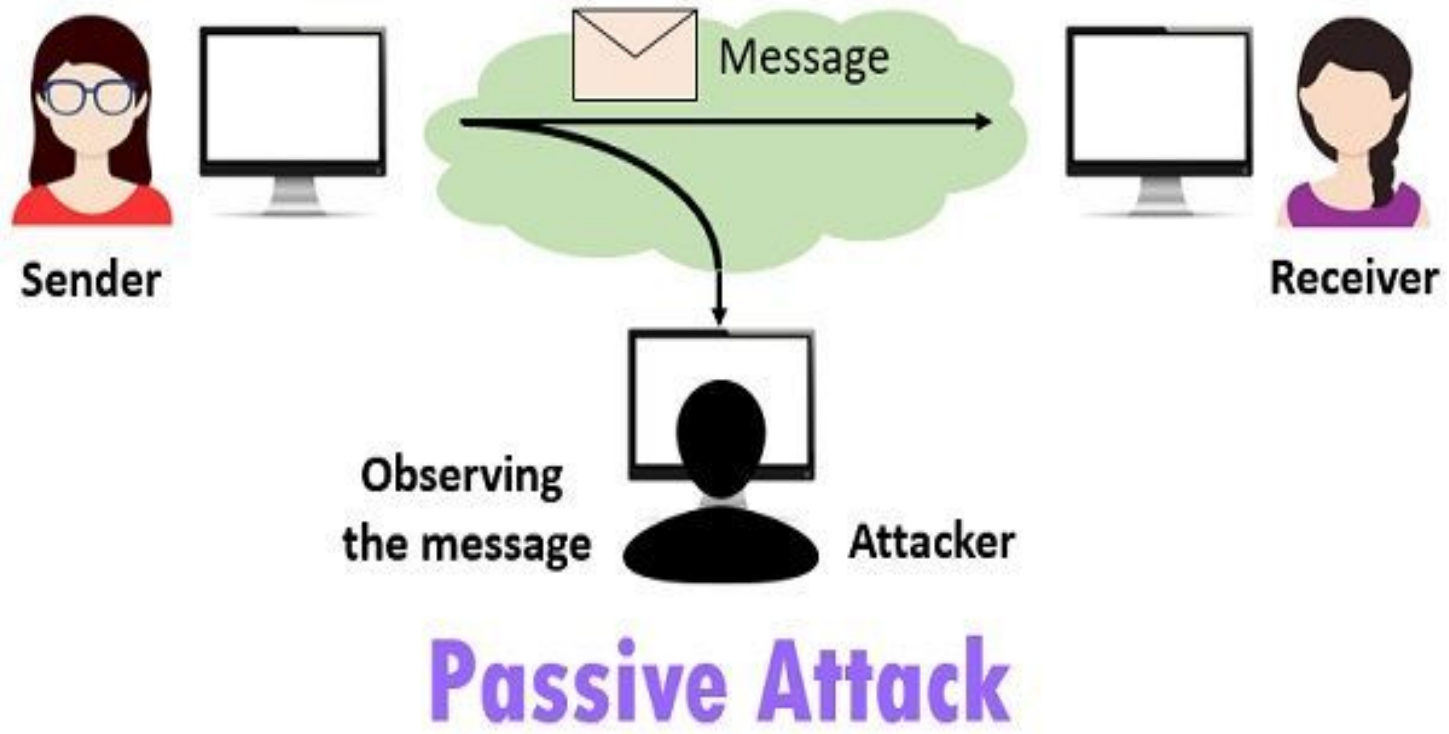


Classification of Attack

Passive Attacks	• Passive attacks do not tamper with the data and involve intercepting and monitoring network traffic and data flow on the target network • Examples include sniffing and eavesdropping
Active Attacks	• Active attacks tamper with the data in transit or disrupt the communication or services between the systems to bypass or break into secured systems • Examples include DoS, Man-in-the-Middle, session hijacking, and SQL injection
Close-in Attacks	• 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 disrupt access to information • Examples include social engineering such as eavesdropping, shoulder surfing, and dumpster diving
Insider Attacks	• Insider attacks involve using privileged access to violate rules or intentionally cause a threat to the organization's information or information systems • Examples include theft of physical devices and planting keyloggers, backdoors, and malware
Distribution Attacks	• Distribution attacks occur when attackers tamper with hardware or software prior to installation • Attackers tamper with the hardware or software at its source or in transit

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.

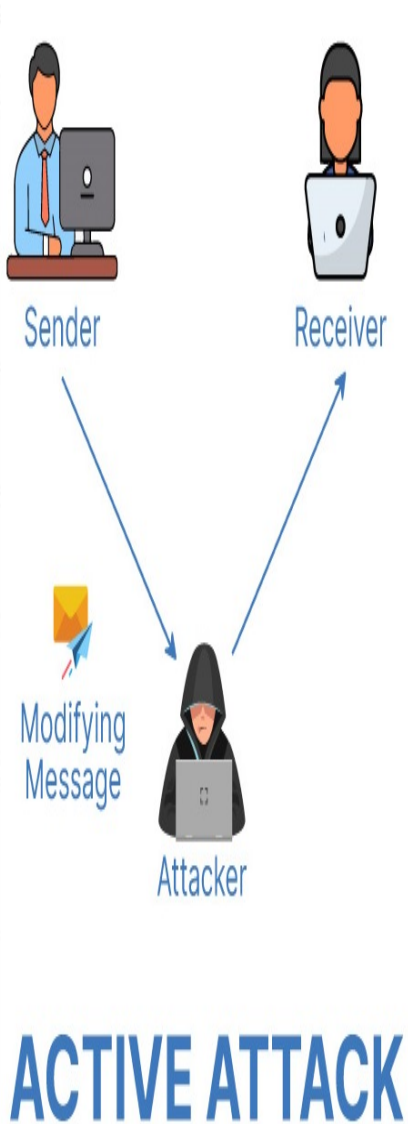


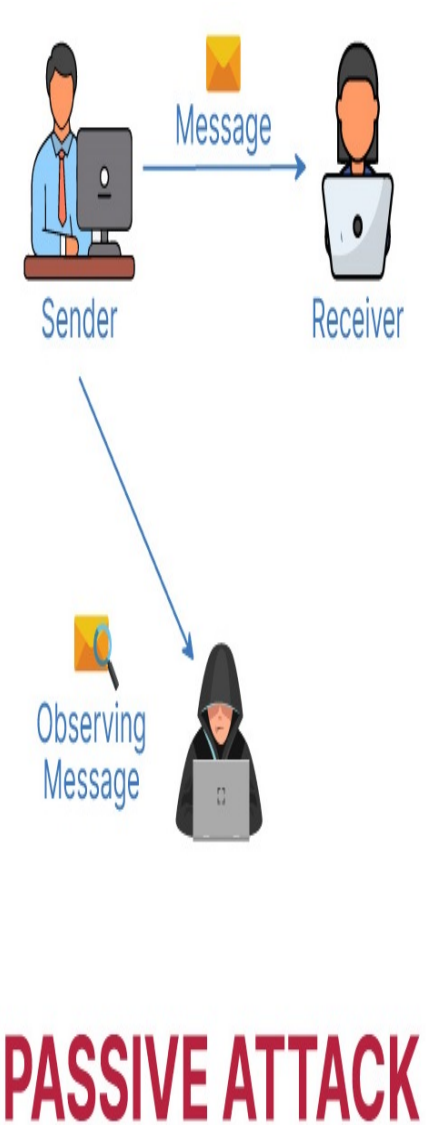
Active Attack

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 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.





Close-in Attack

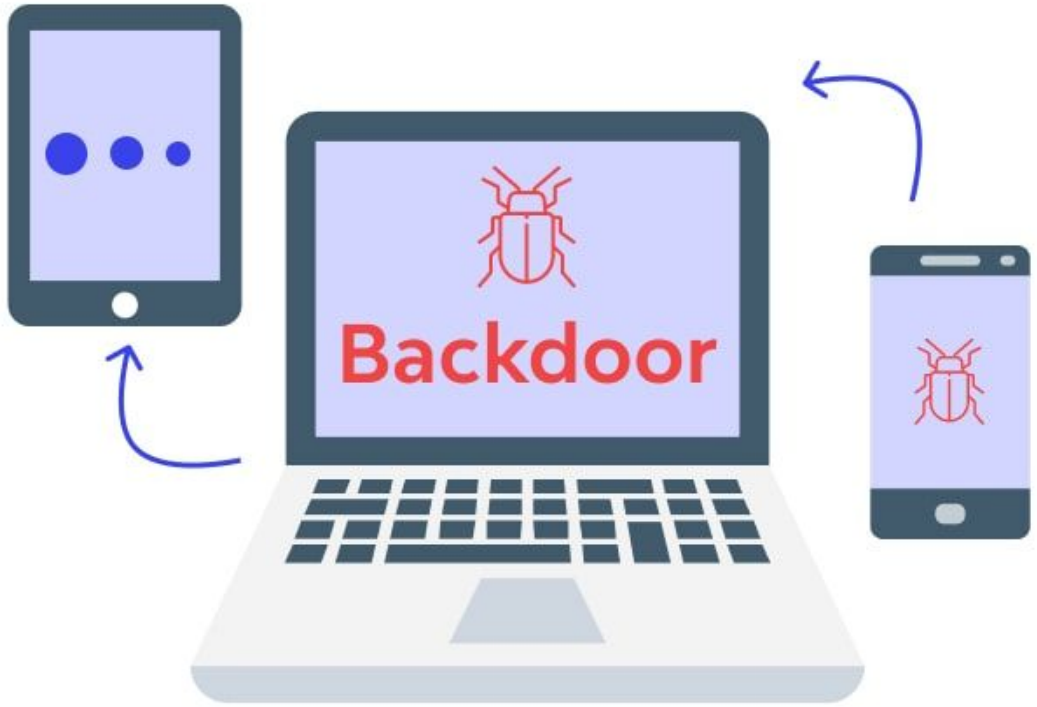
A Close-in attack is a type of attack where the attacker is physically close to the target system. Attacker can the the advantages of being physically close to the target devices.

Insider Attack

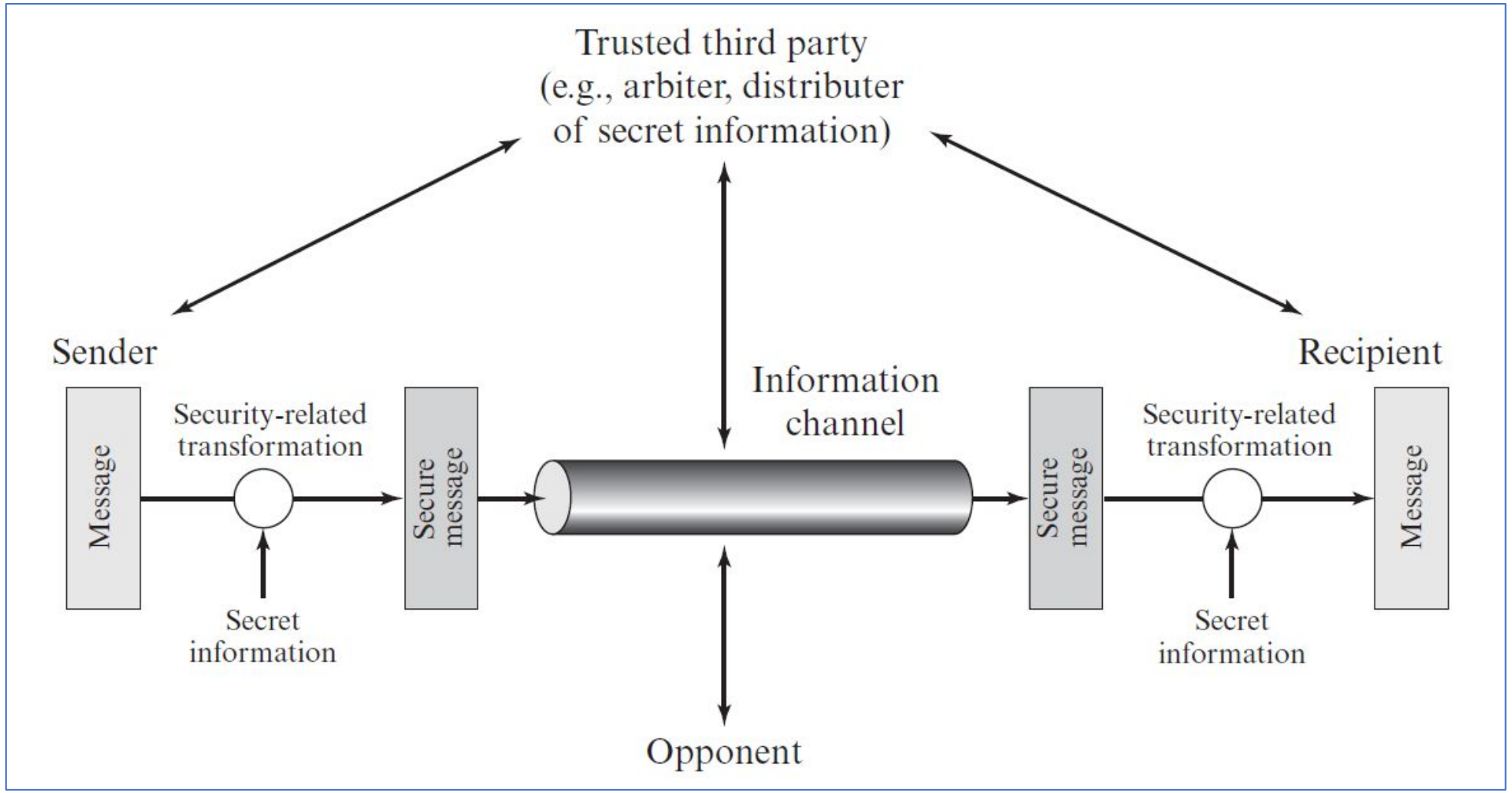
An insider attack is an attack from inside users (a person with authorized system access.), who use their access credentials and knowledge of the network to attack the target machines.

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

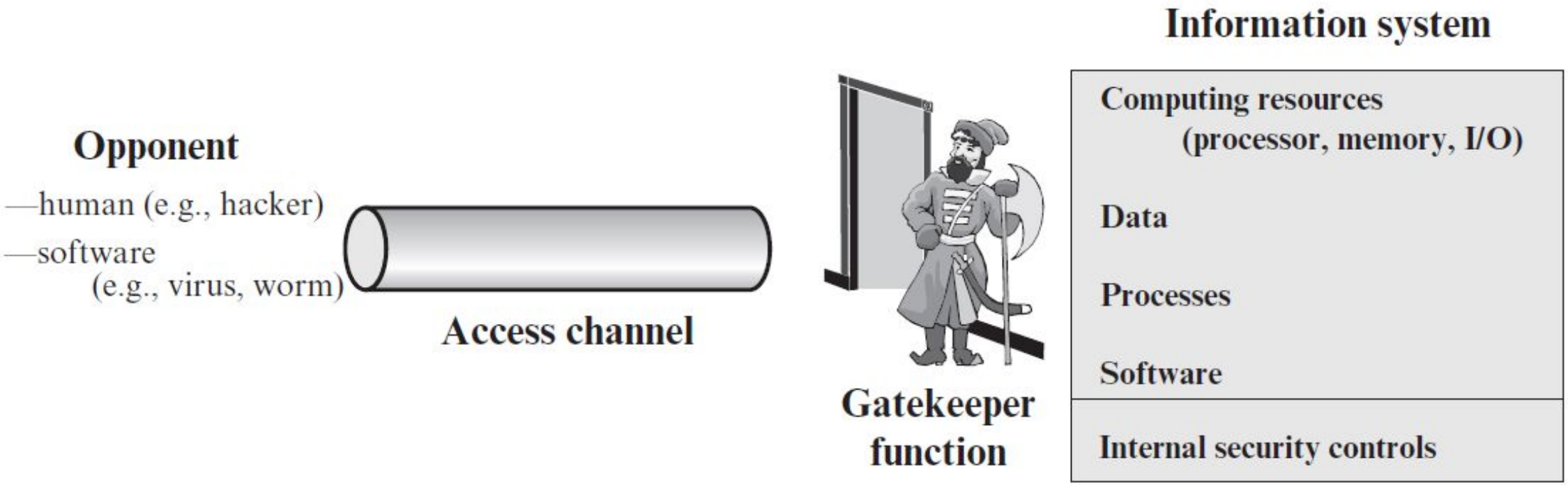
- Upon receipt, the Recipient performs another security-related transformation of the message (called ***Decryption***) to convert the secure message to the original message. The Recipient uses some secret information (called Key) for the conversion.

- 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.

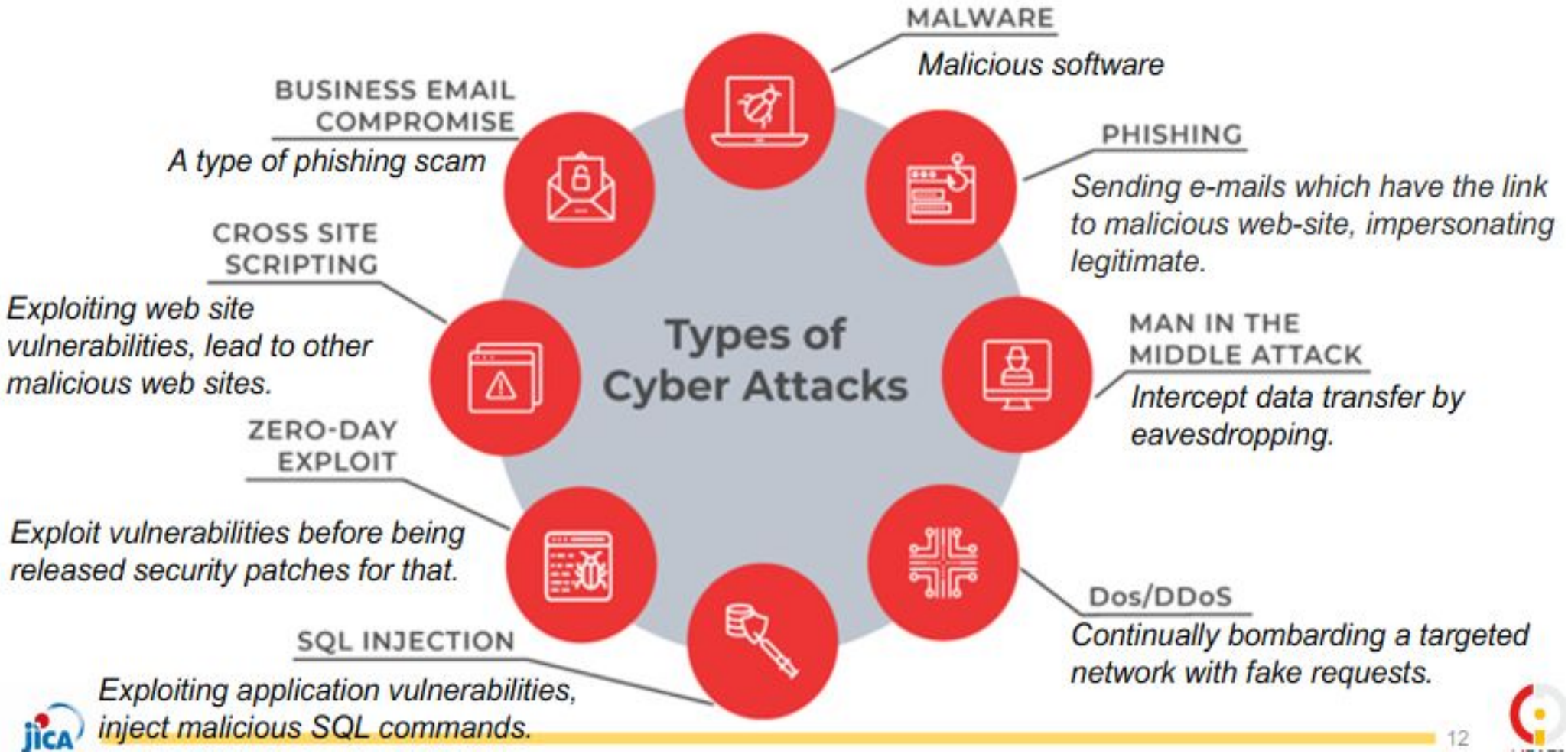
Model for Network Access Security



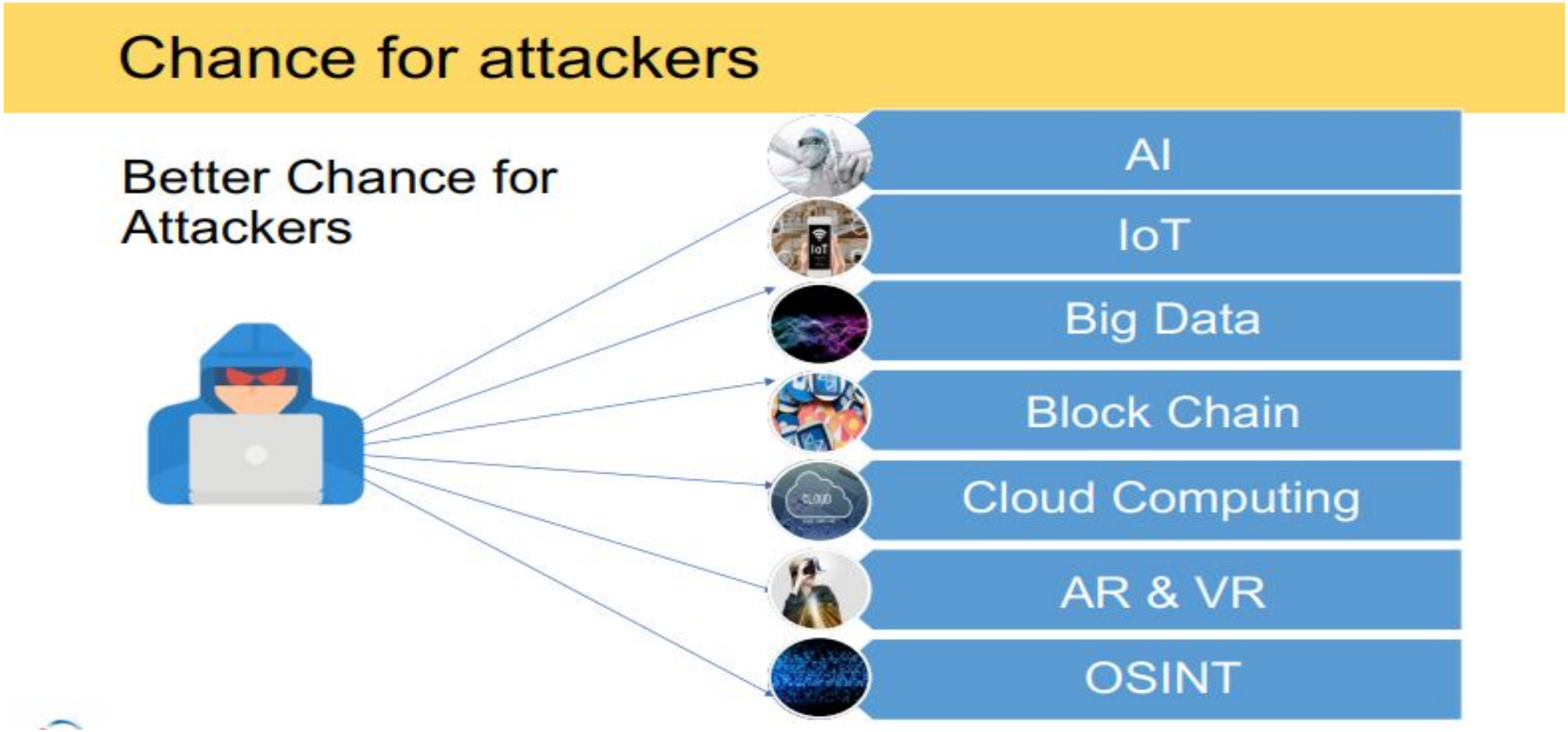
Model for Network Access Security

- **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.

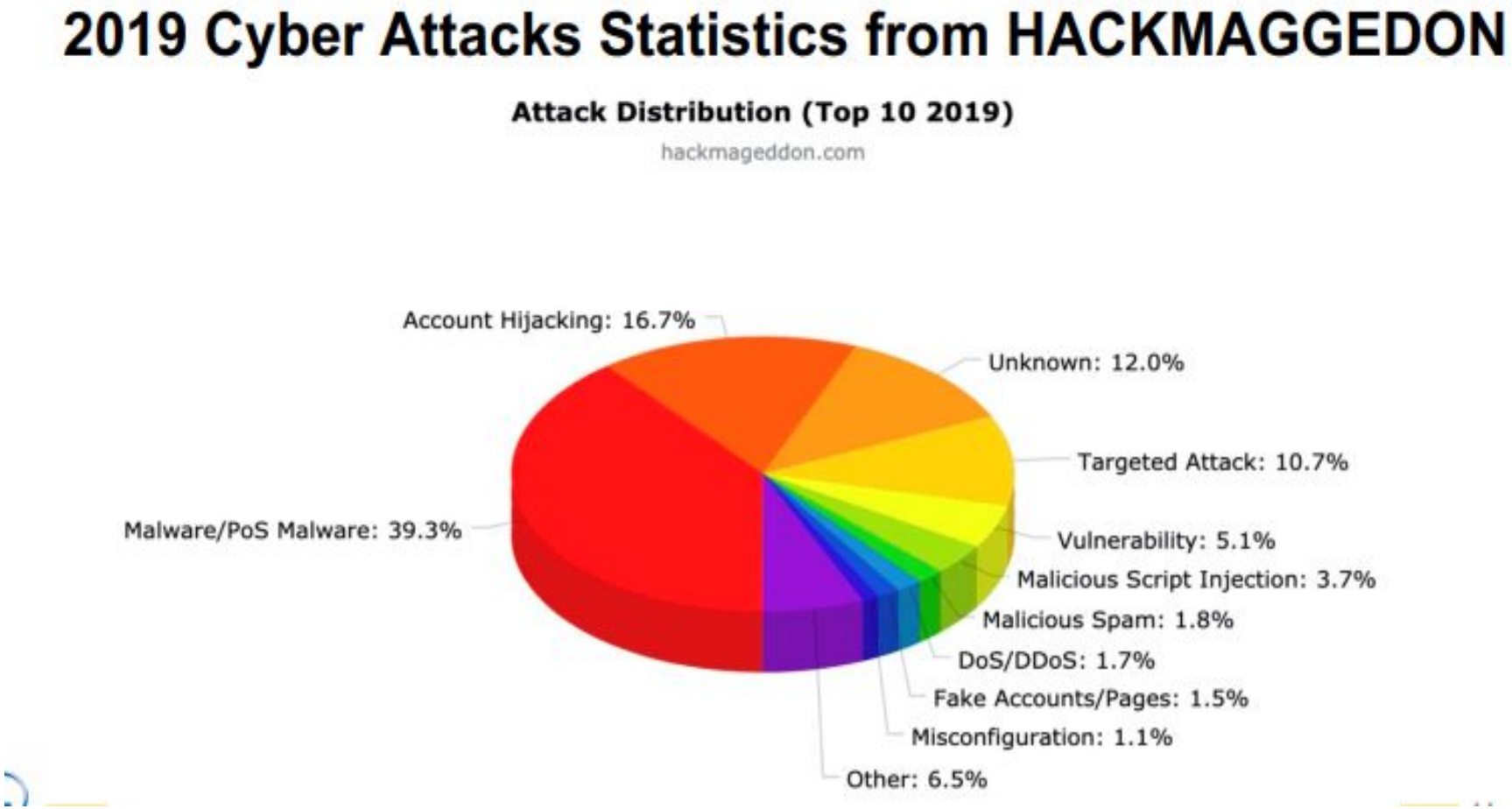
Cyber Attacks



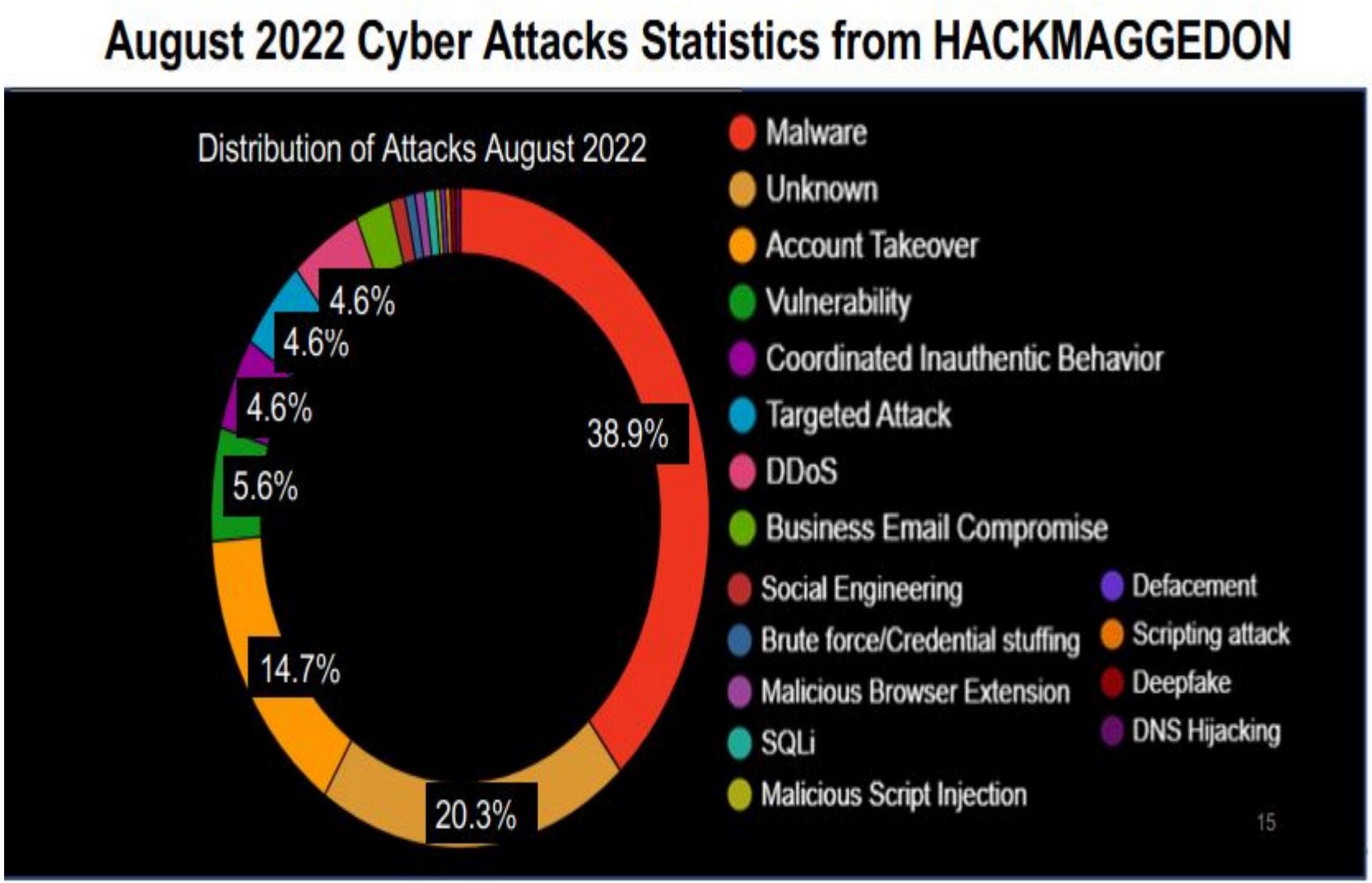
Chance Cyber Attacks



Trend of Cyber Attacks



Trend of Cyber Attacks

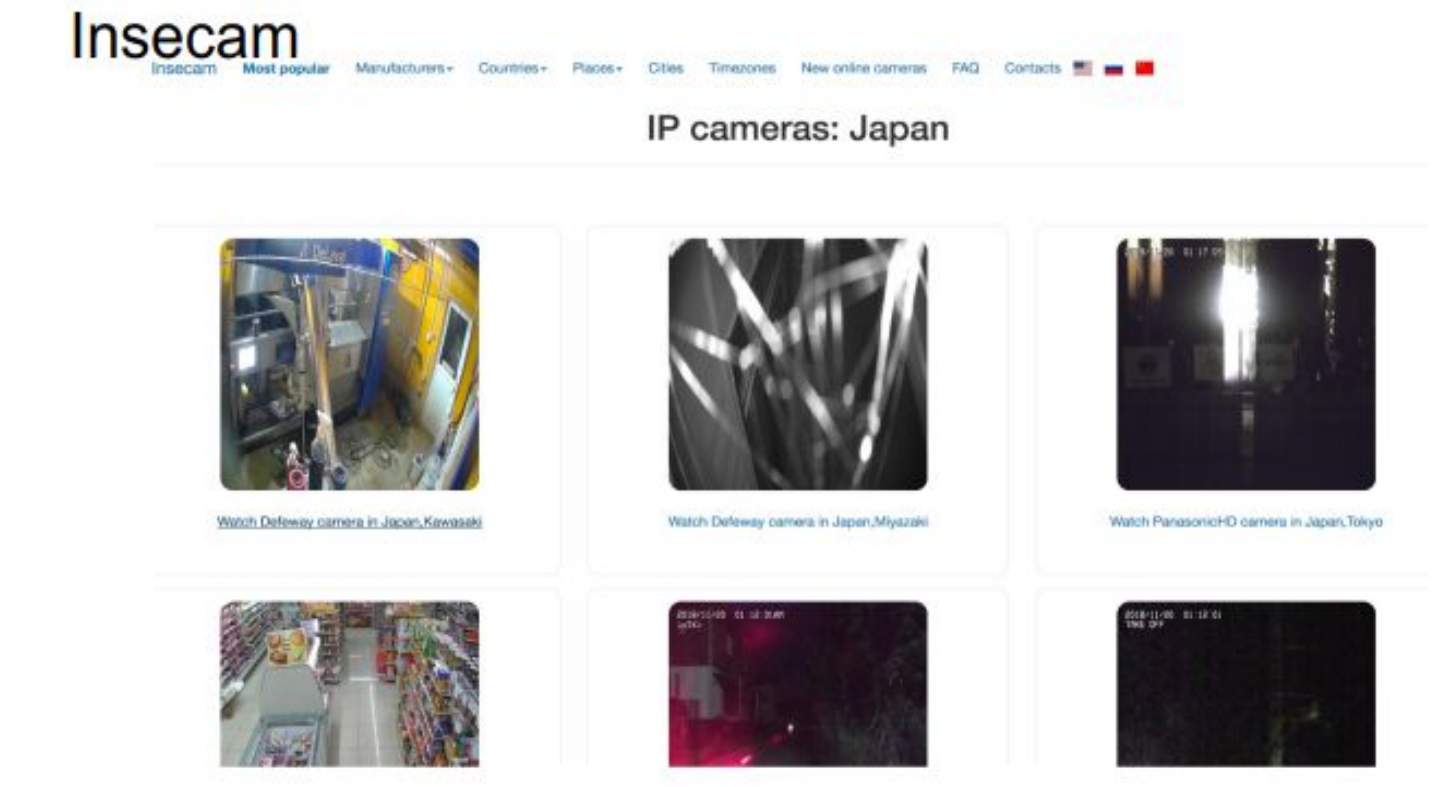


Impact of cyber attack

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

Show some Leaked Data as Demo

Understanding Cyber-attack Situation

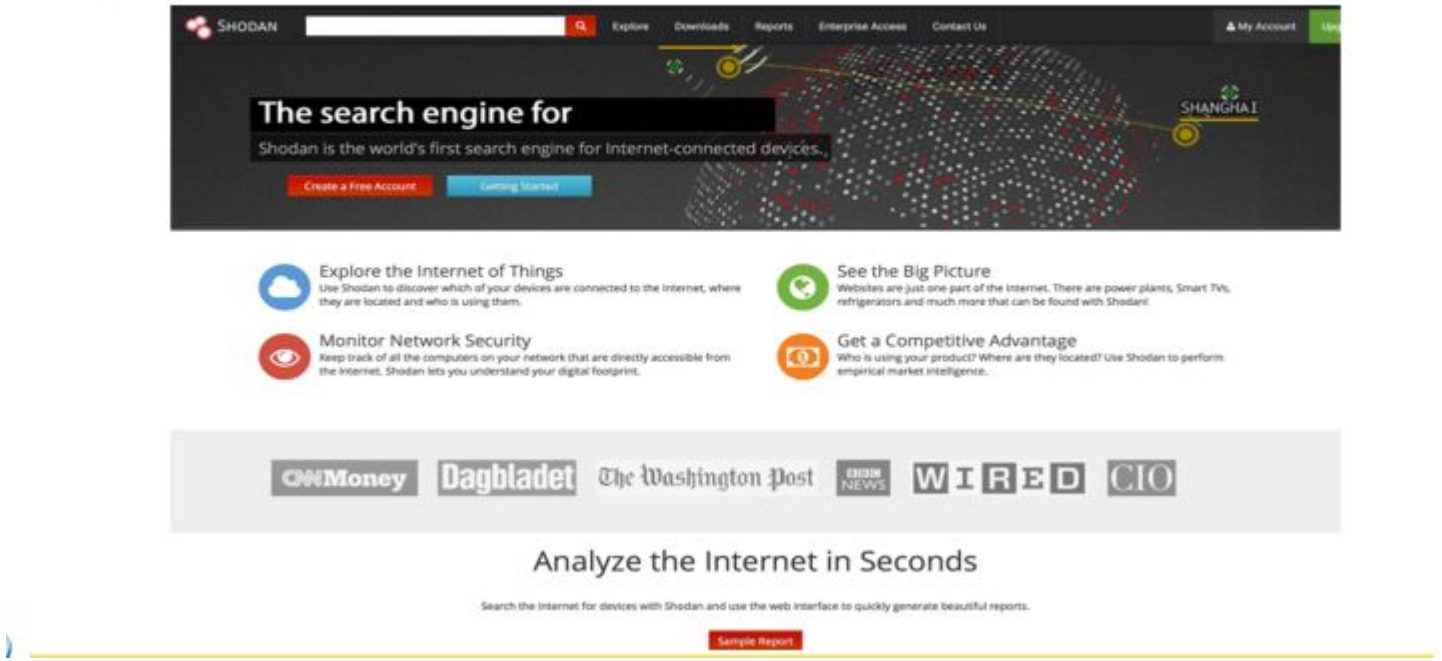


Understanding Cyber-attack Situation

http://exploit-db.com

Understanding Cyber-attack Situation

http://shodan.io



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

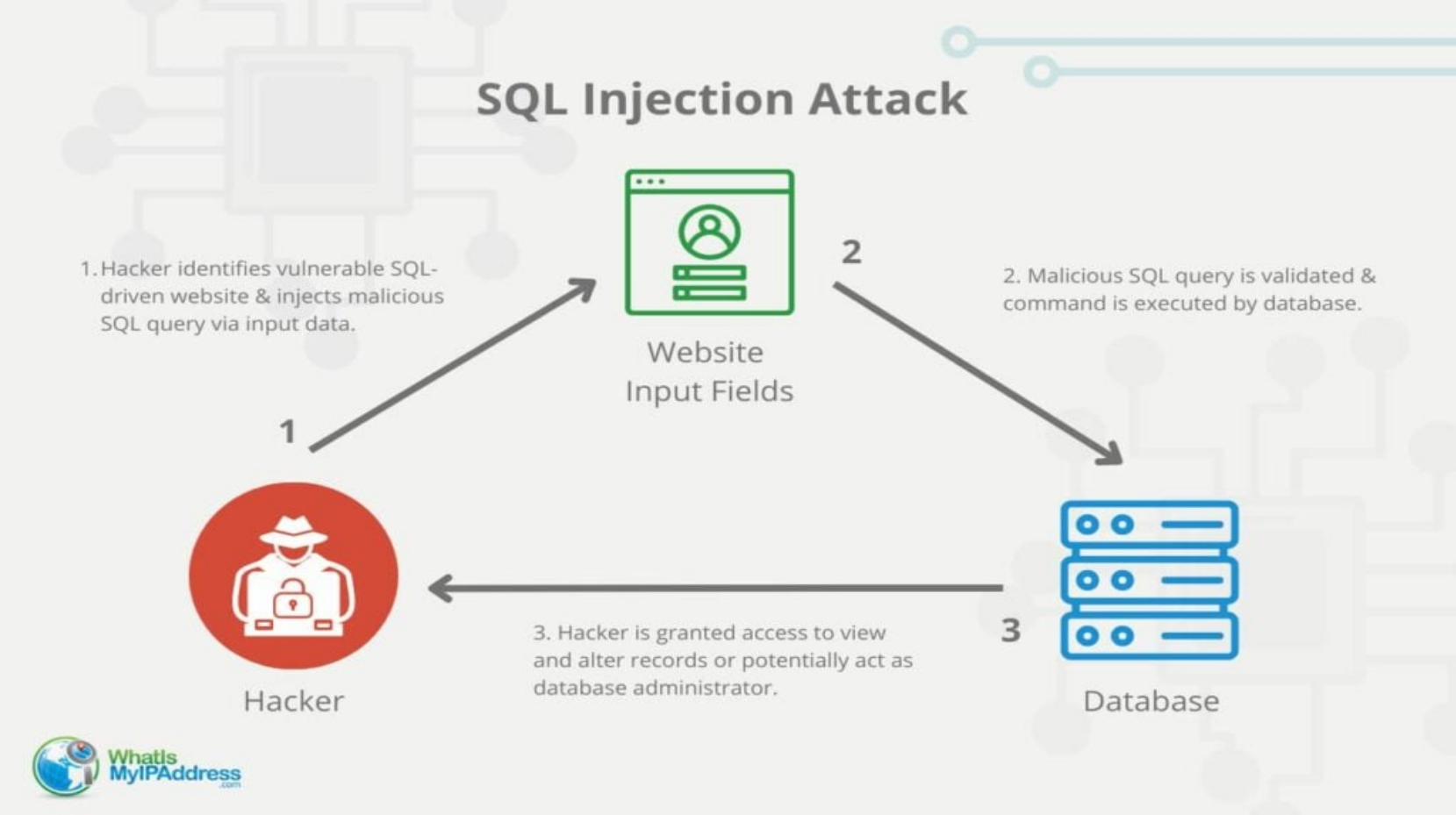
Web-based Attacks

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

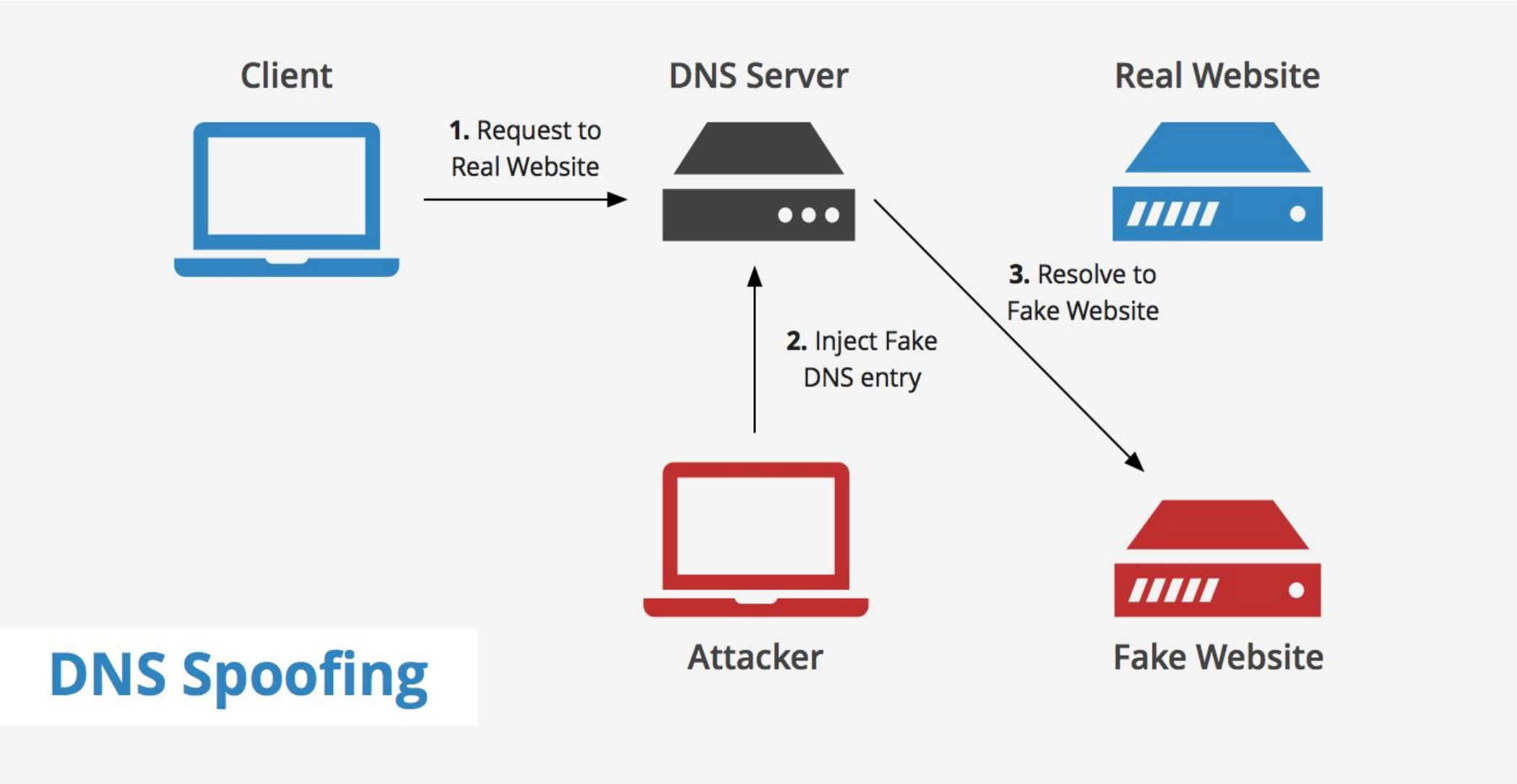
- ✔ **Injection attacks**
- ✔ **DNS Spoofing**
- ✔ **Session Hijacking**
- ✔ **Phishing**
- ✔ **Brute force**
- ✔ **Denial of Service**
- ✔ **Dictionary attacks**
- ✔ **URL Interpretation**
- ✔ **Zero-Day Exploit**
- ✔ **File Inclusion attacks**
- ✔ **Man in the middle attacks**
- ✔ **Cross-site scripting**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

Injection Attack

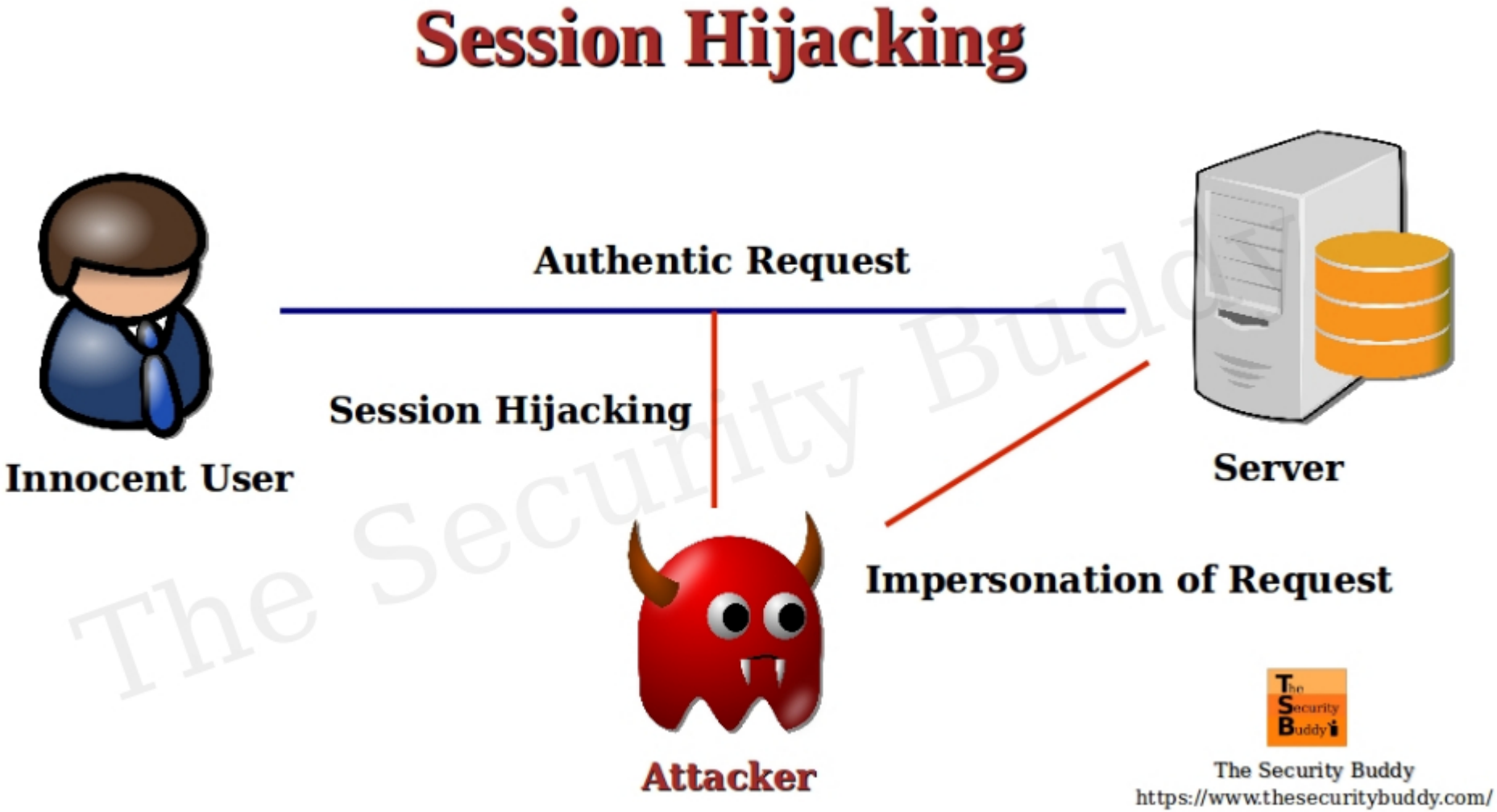
This type of attack allows an attacker to inject code into a program or query or inject malware onto a computer in order to execute remote commands that can read or modify a database or change data on a web site.



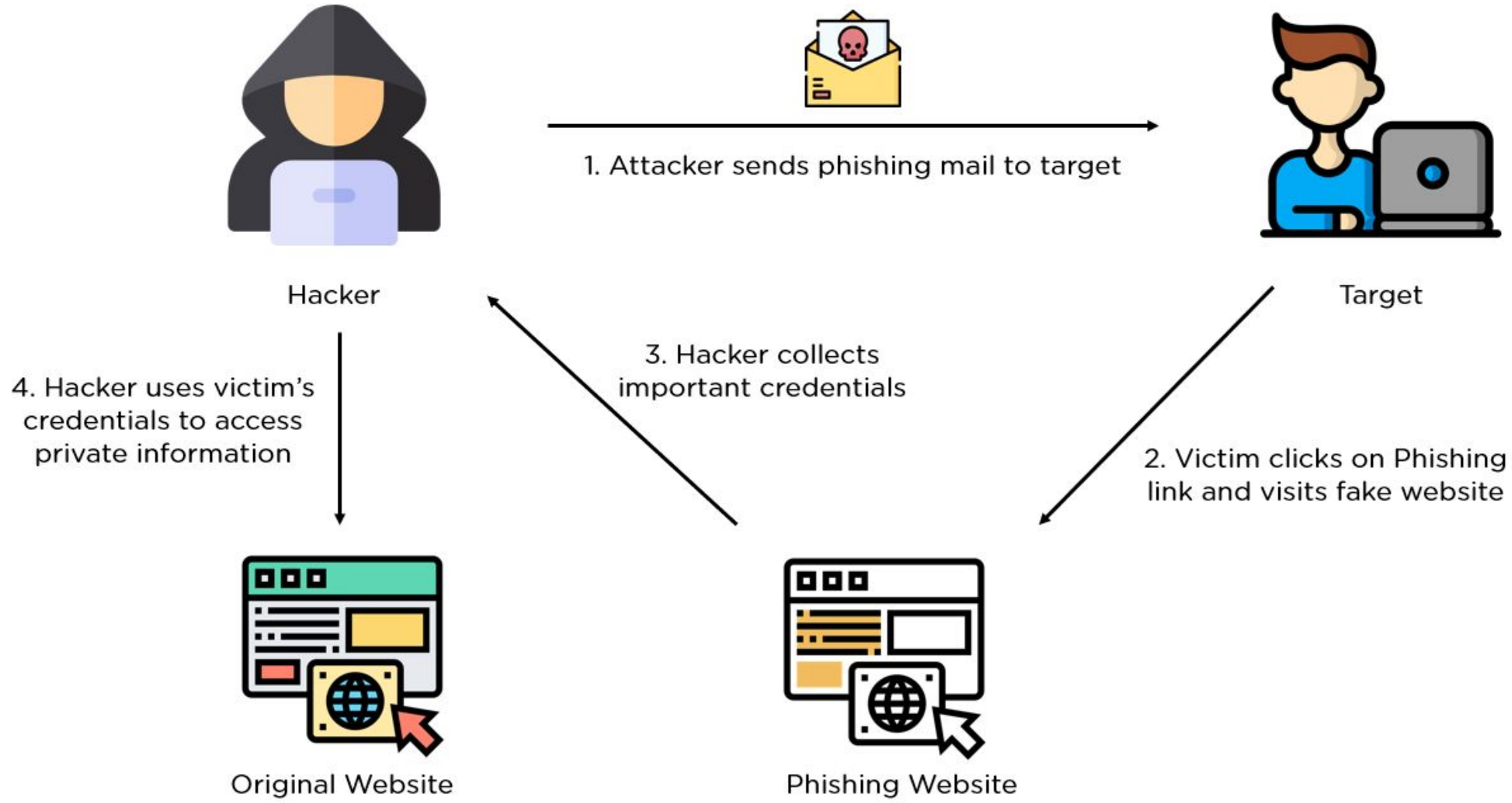
DNS Spoofing



Session Hijacking



Phishing


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

Brute Force

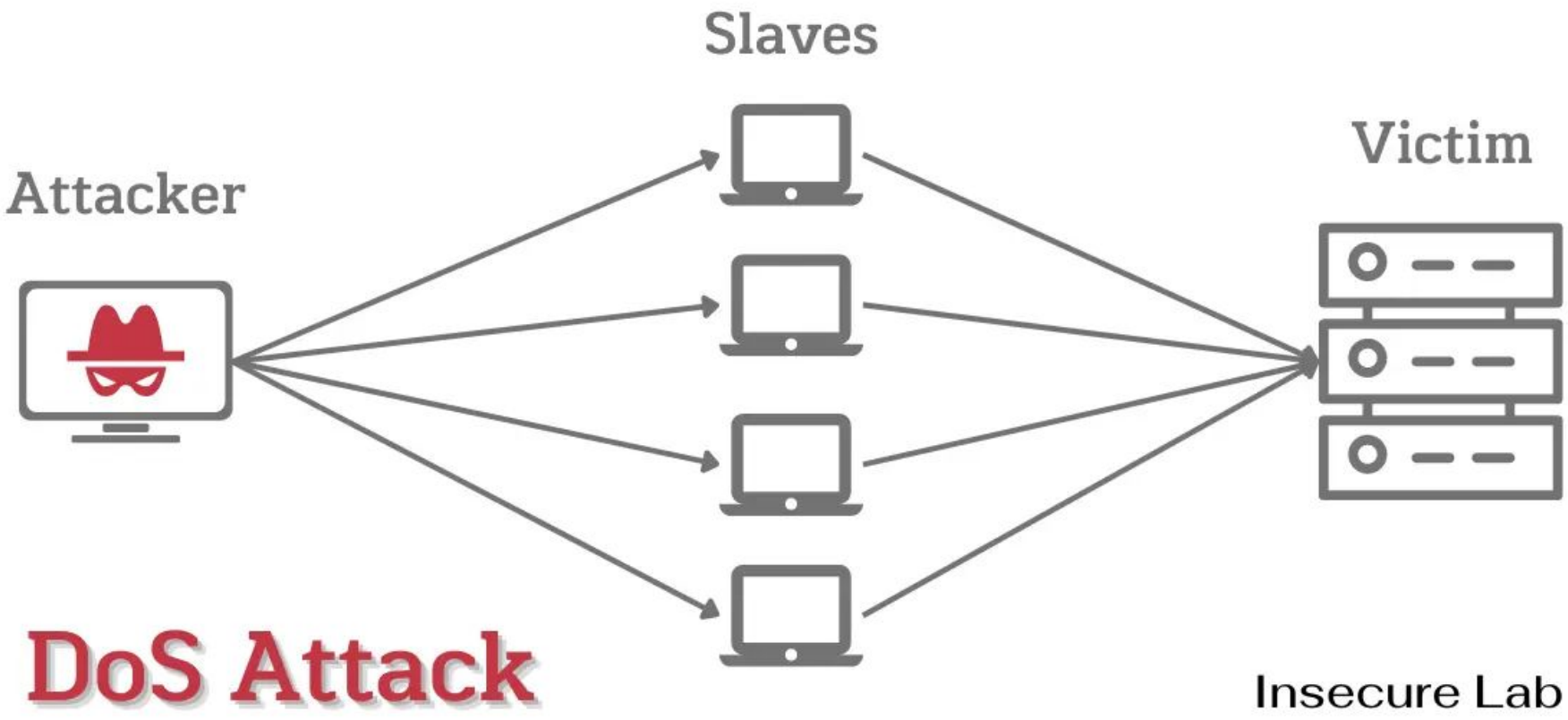
Attacker

Guess List Of Username & Password Combination

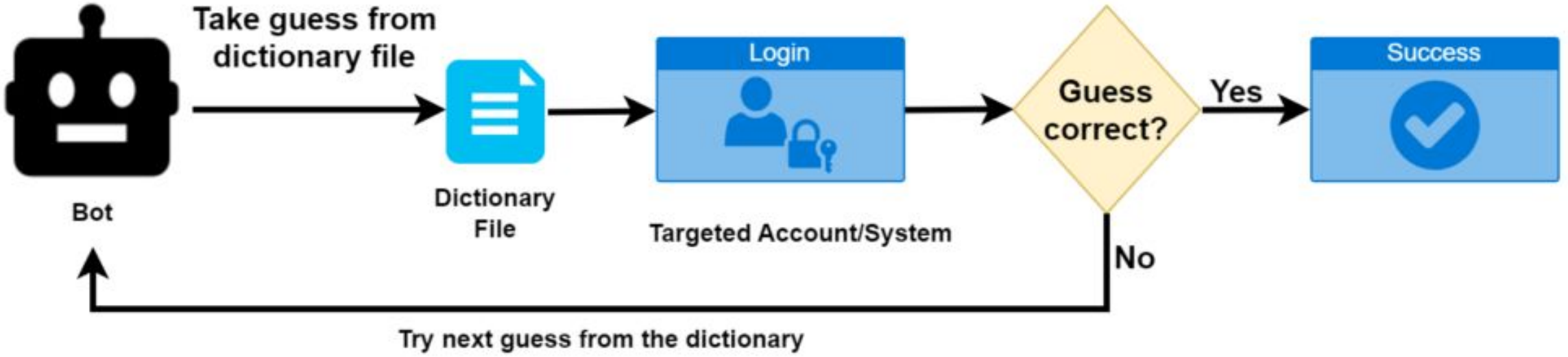
Repeats Login Attempts Until One Is Successful

Successful Credential Validation

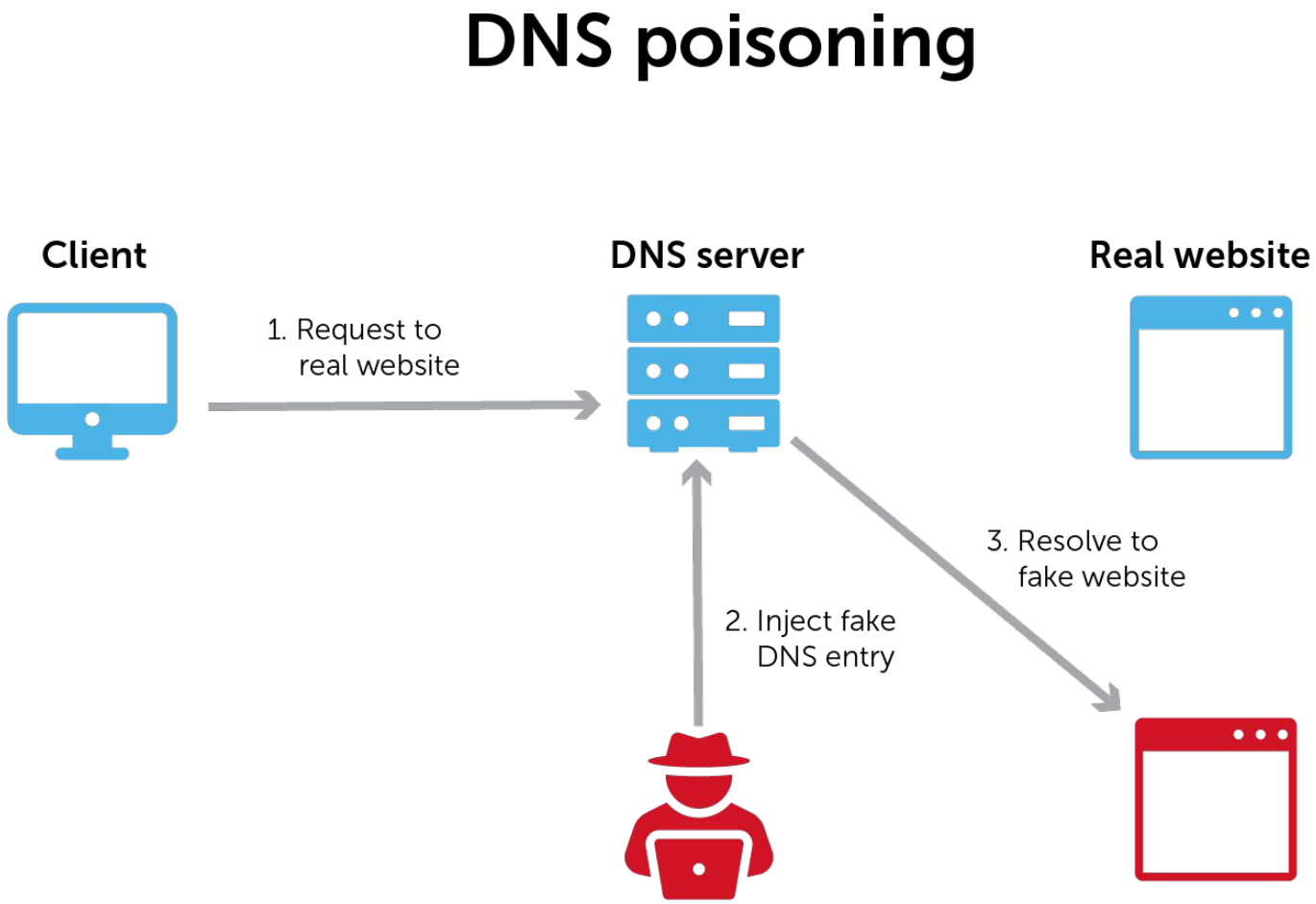
Denial of Service (DoS) Attacks



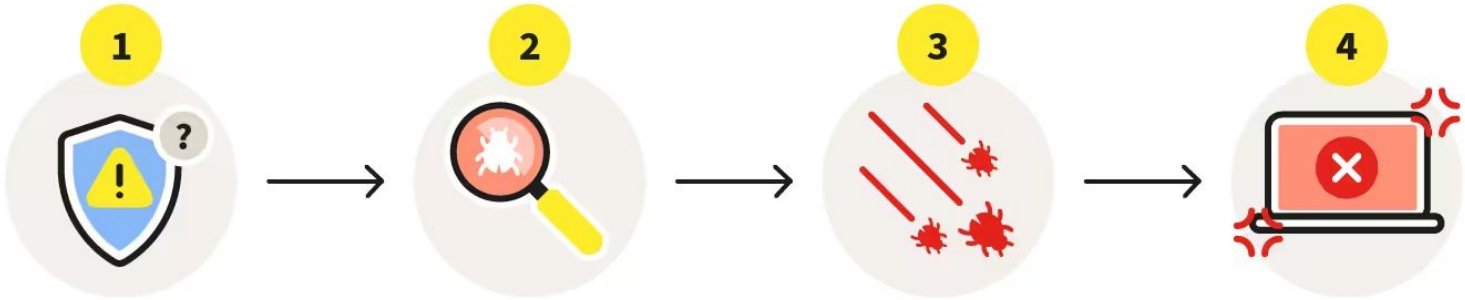
Dictionary Attacks



URL Interpretation



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.

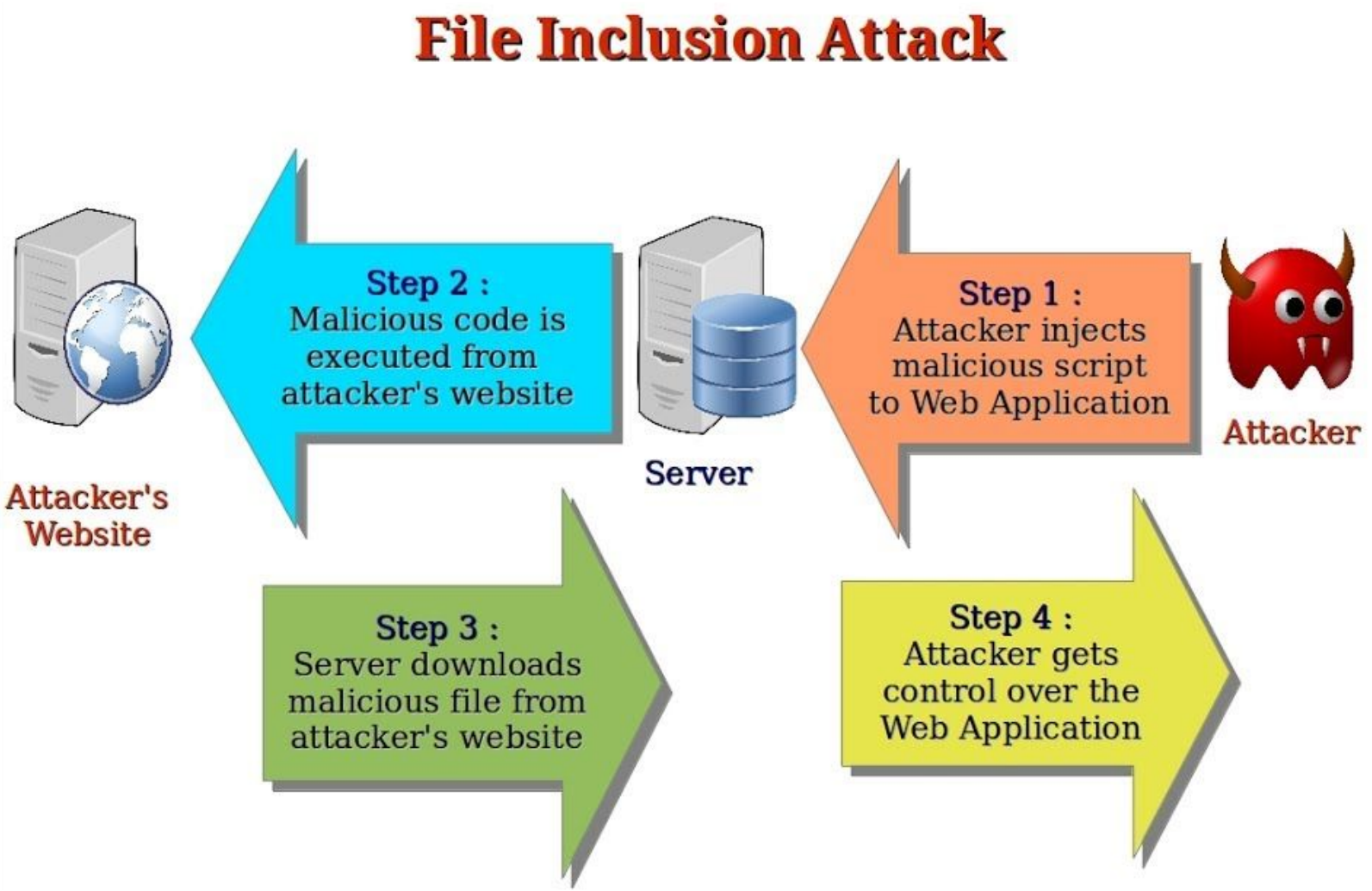
3

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

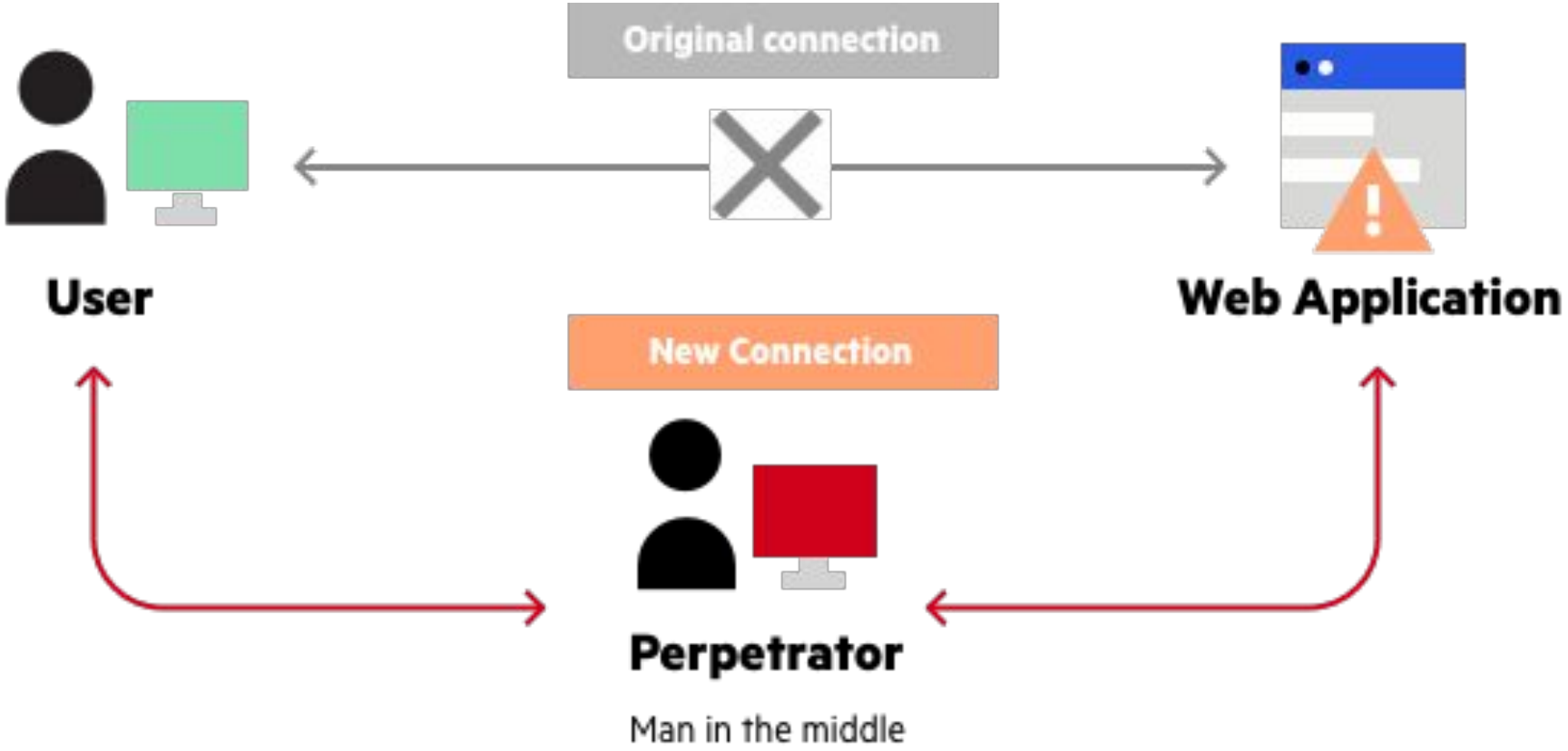
4

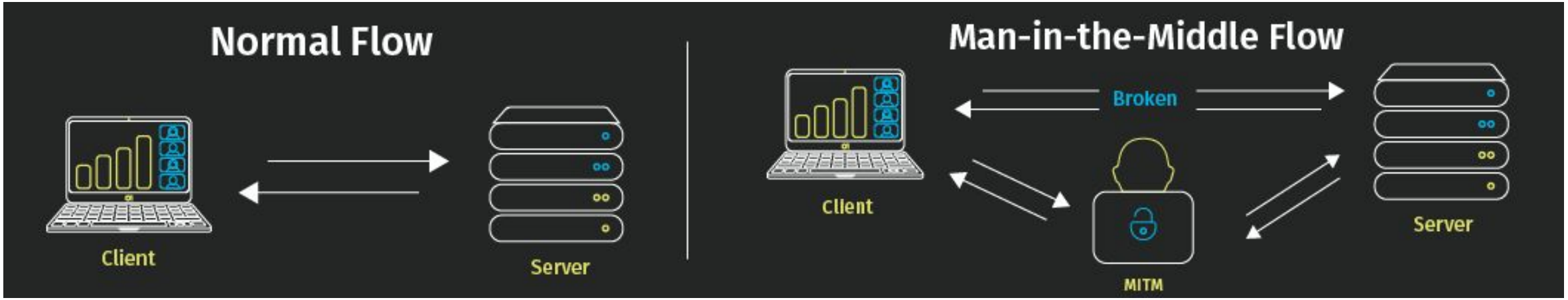
Developers detect the attack and have zero days to mitigate it.

File Inclusion Attacks

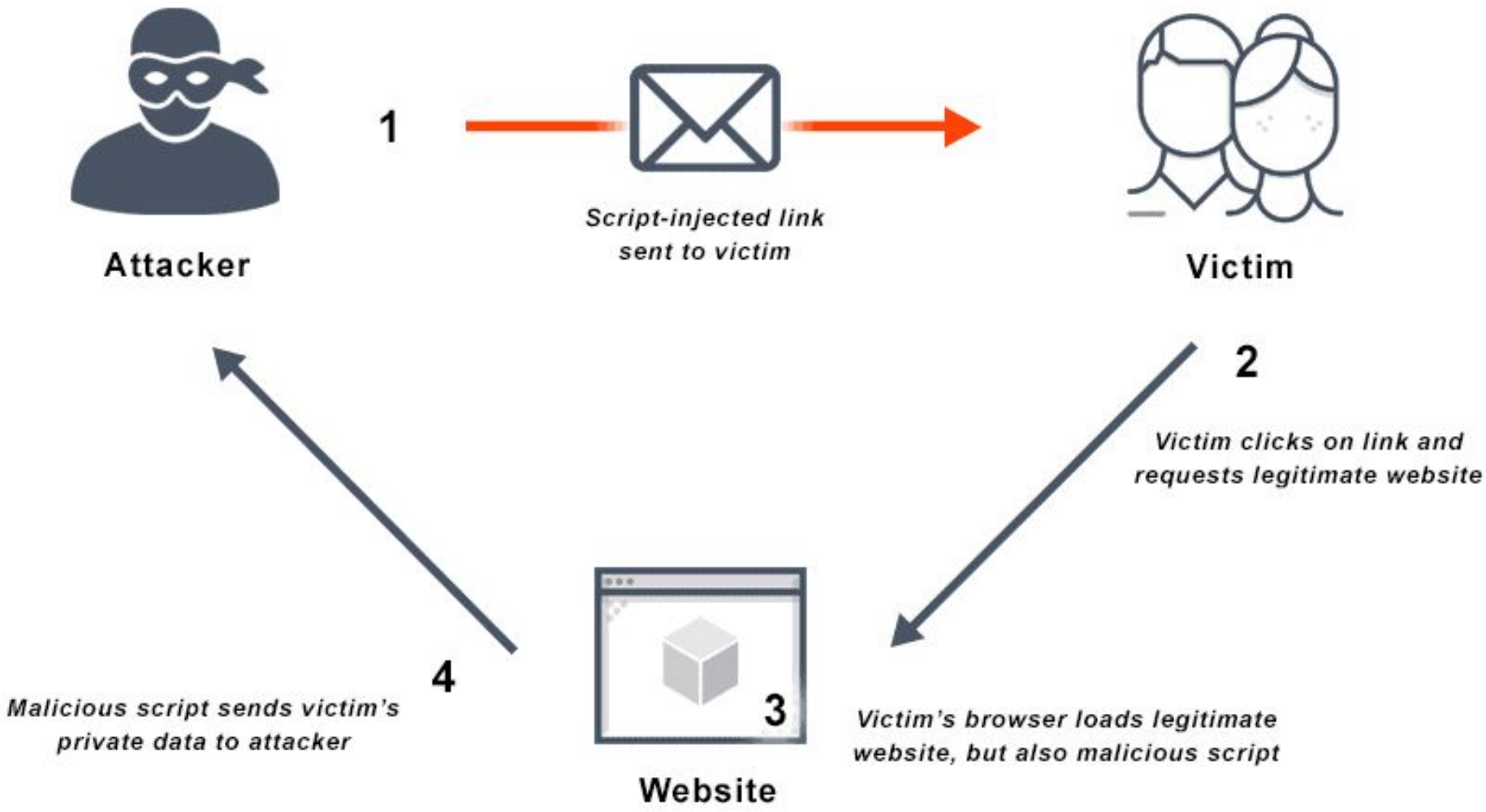


Man in the Middle Attacks

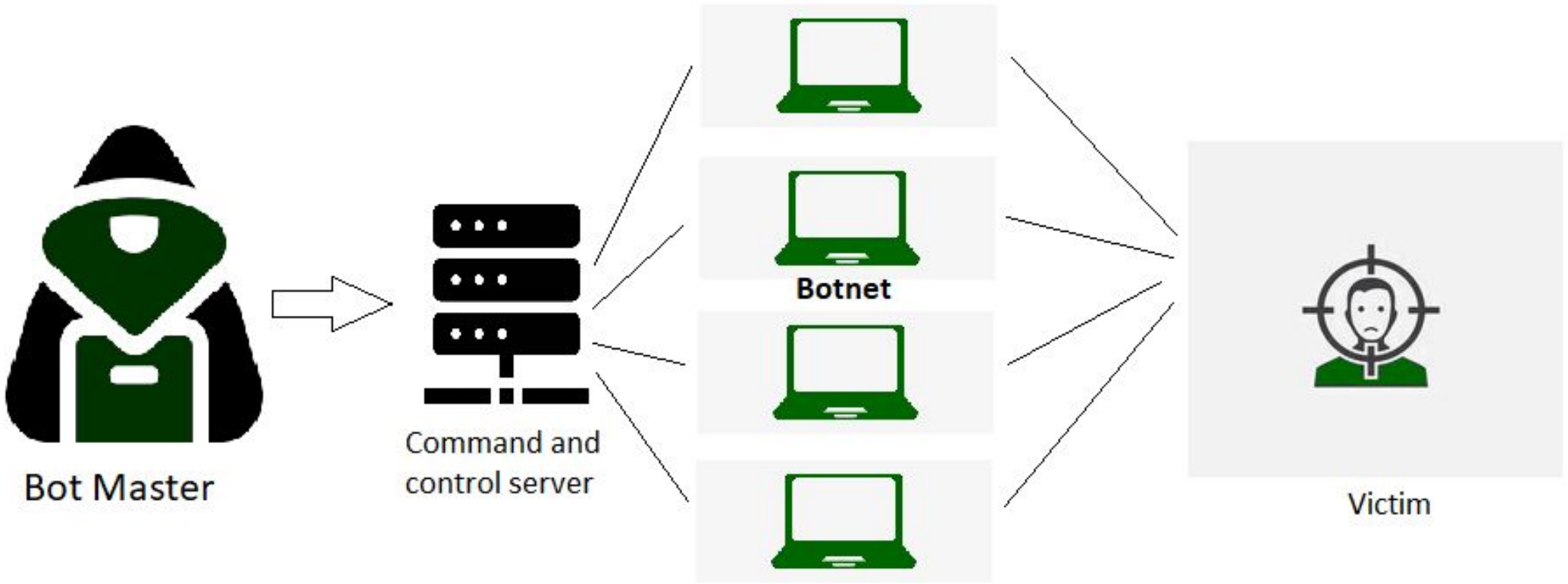




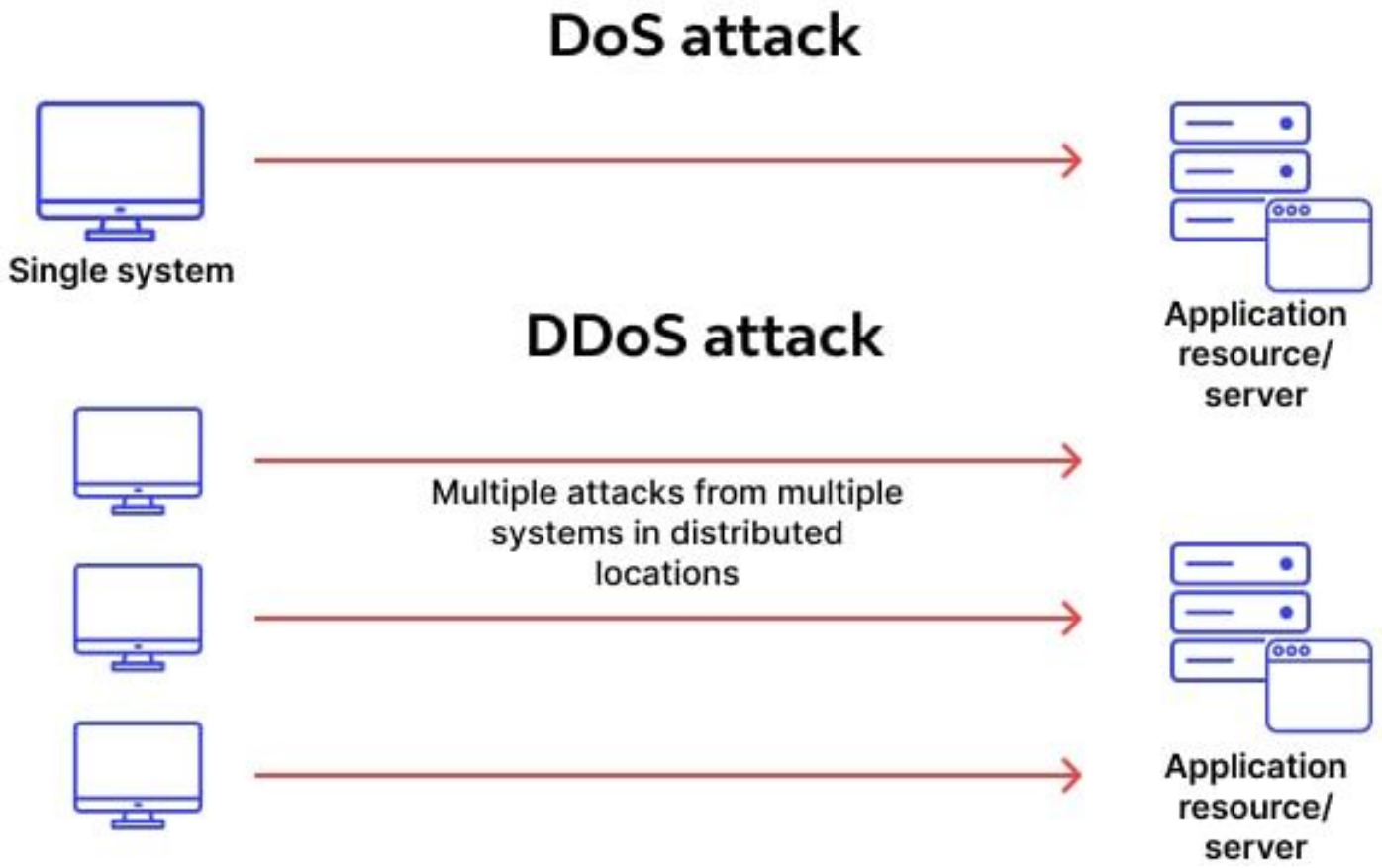
Cross-Site Scripting



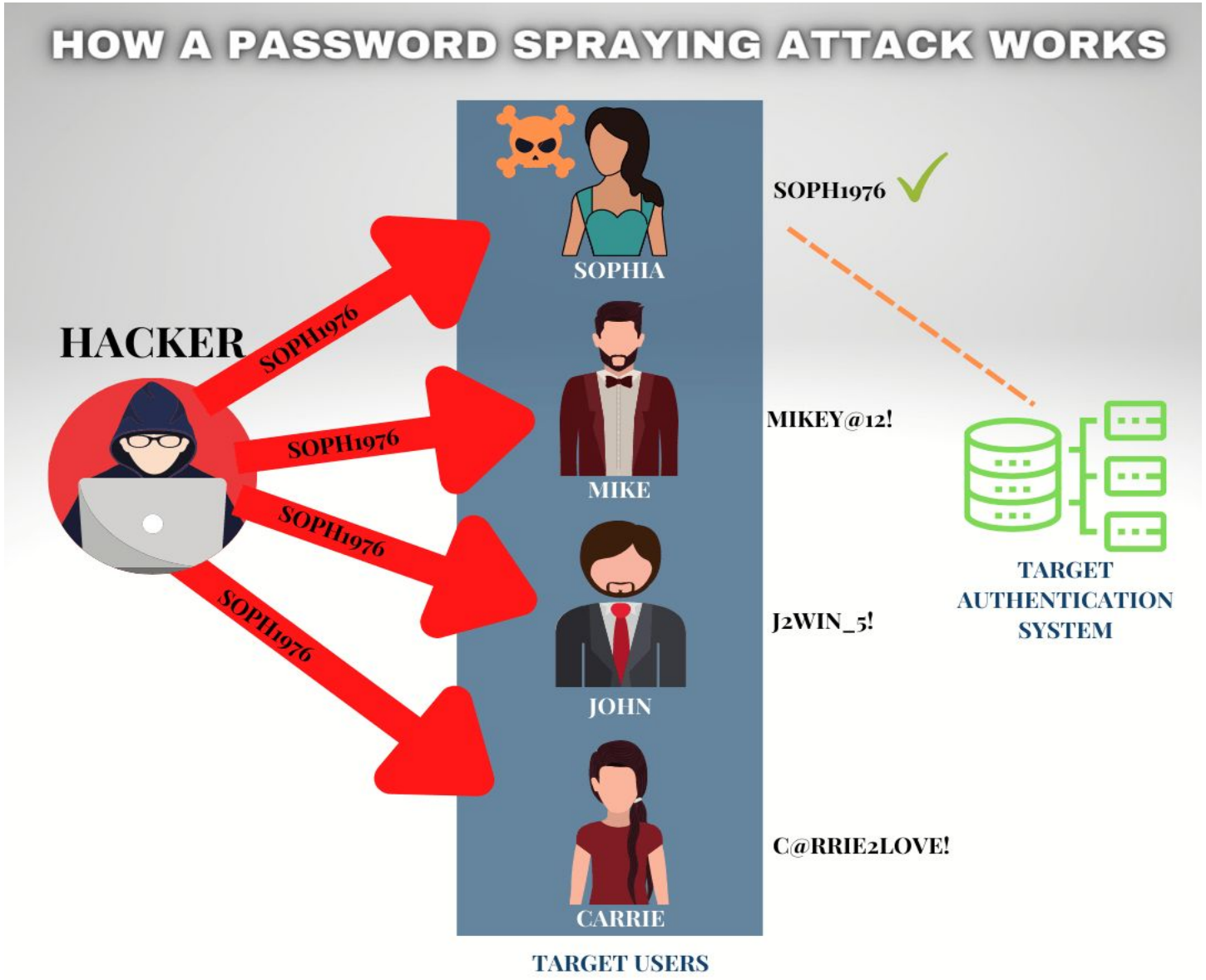
Distributed Denial of Service (DDoS) Attacks



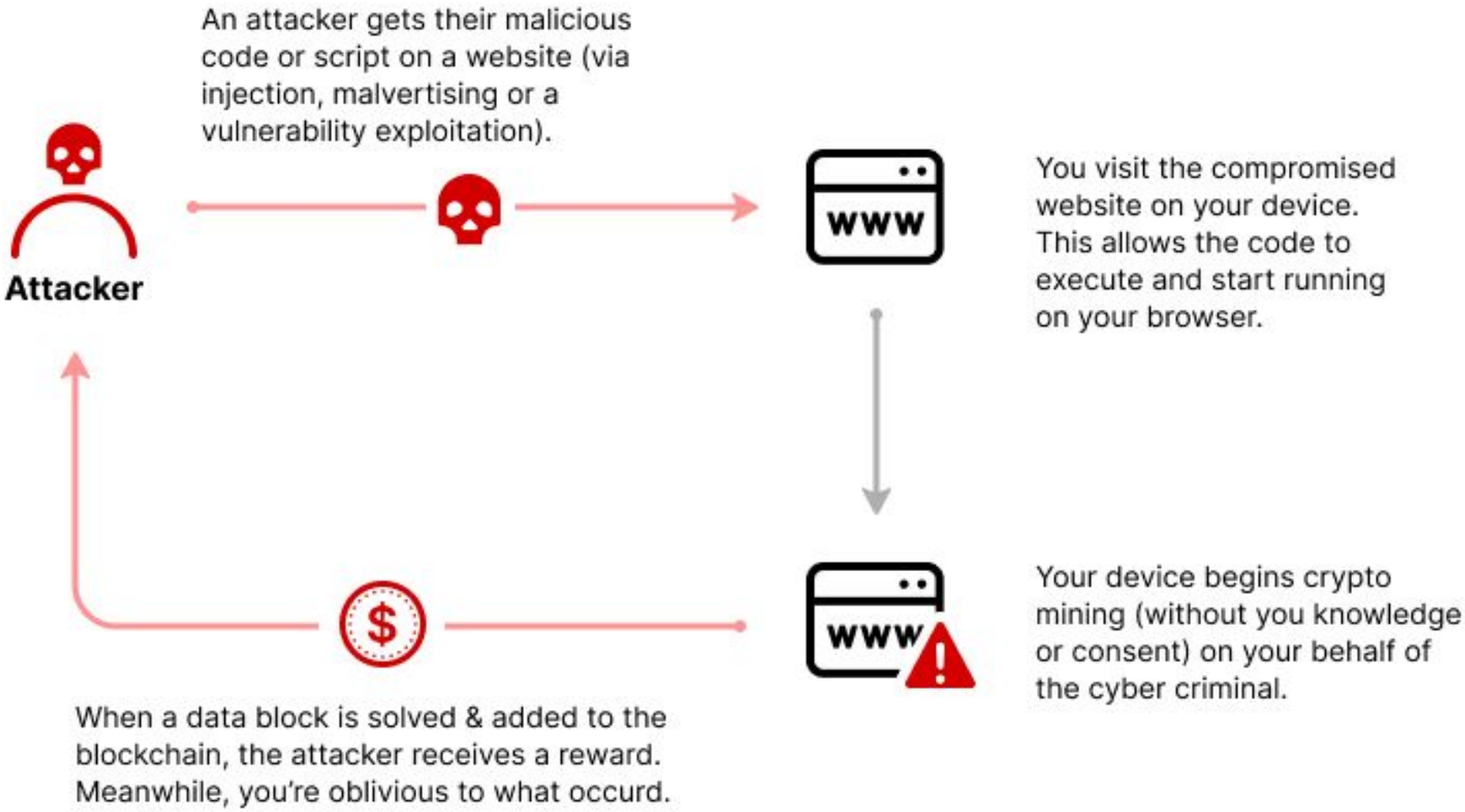
DoS vs. DDoS Attacks



Password Attack



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

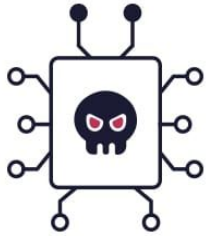
Phishing emails
file attachme

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

Different ways malware can enter your network

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

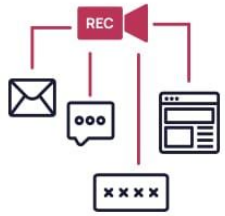
ADWARE
Spams you with ads

RANSOMWARE
Encrypts files and blackmails you

FILELESS MALWARE
Operates in your system's memory

ROOTKIT
Gives remote access to your device

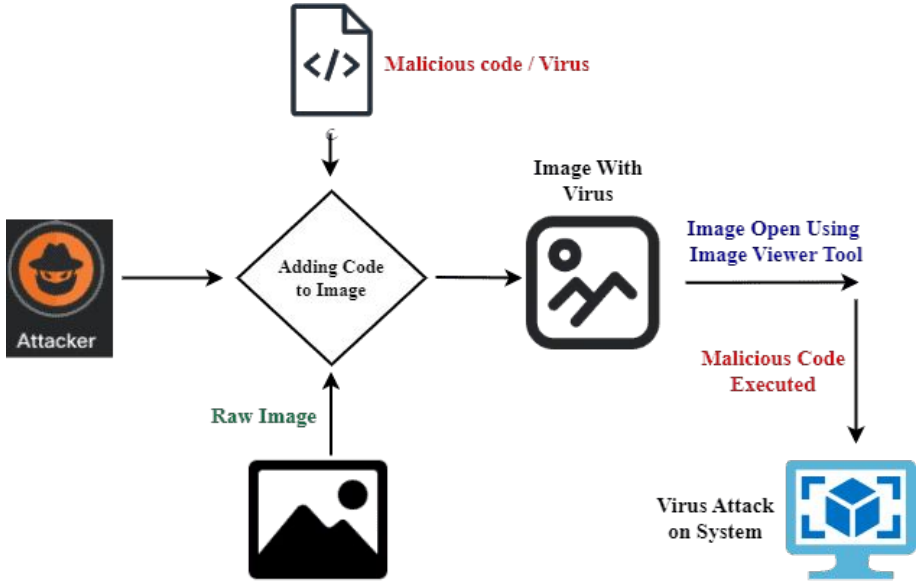
BOTNET
Turns your PC into a puppet



KEYLOGGER
Records user activity

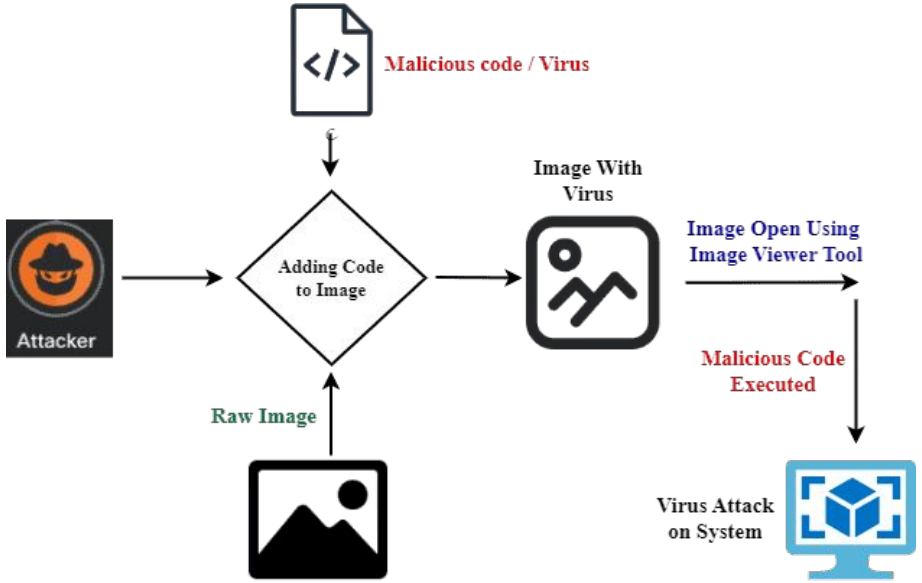
Viruses

- 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.

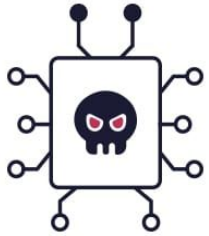


Viruses

- 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

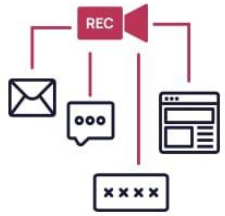
ADWARE
Spams you with ads

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