HACKER COMBAT
COMMUNITY

What is a Man-in-the-Middle Attack and How To Avoid It?

Learn More about this Common, Potent, and Devastating Cyber attack

Hackercombat.com

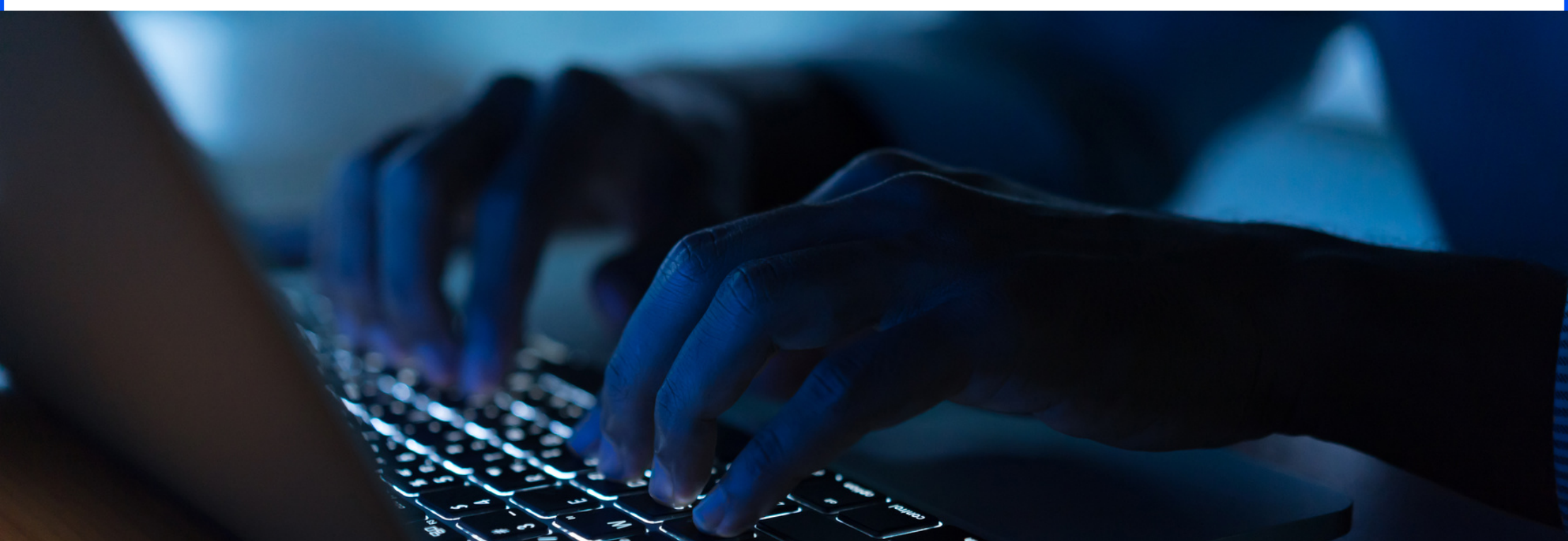
What is a Man-in-the-Middle (MITM) Attacks – Definition

MITM attack refers to the kind of cyberattack in which an attacker eavesdrops on the communication between two targets- two legitimately communicating hosts- and even hijacks the conversation between the two targets.

Thus, the attacker is able to “listen” to a conversation that he is not supposed to listen to and even alter the course of the communication, remaining invisible and undetected all the while.

The attacker can thus gather information, including personal data, from either participant and can even execute malicious activities, including launching a malware attack.

A typical MITM (Man in the Middle) Attack is just like getting in between a telephone conversation, remaining transparent and at the same time interacting with both the participants posing as the person at the other end.



Techniques Used In (MITM) Man-in-the-Middle Attacks

HACKER COMBAT COMMUNITY

Sniffing

Hackers put some wireless devices on monitoring mode and thus are able to sniff out packets that they are not intended to see. Thus, they can sniff out or see packets meant for other hosts and use the same to hijack communication.

@hackercombat

Packet Injection

Hackers inject malicious packets into streams of communication by exploiting the monitoring mode of devices. Such injected packets eventually behave like valid packets and can be used for malicious activities.

Session Hijacking

Hackers sniff sensitive traffic, identifies the temporary session token that's generated for a user and then use the session token to make requests to the user. Once the session token is identified, there's no need to do any further spoofing to hijack a session.

SSL Stripping

Hackers intercept packets, alter their HTTPS-based address requests to go instead to their HTTP equivalent endpoint. Thus, the host ends up making unencrypted requests which eventually leads to sensitive data being leaked in plain text.

Follow us

Visit

Hackercombat.com

SWIPE

HACKER COMBAT
COMMUNITY

How To Prevent MITM Attacks

- Having strong WEP/WAP encryption mechanism on wireless access points.
- Creating a secure environment by using a VPN (Virtual Private Network).

@hackercombat

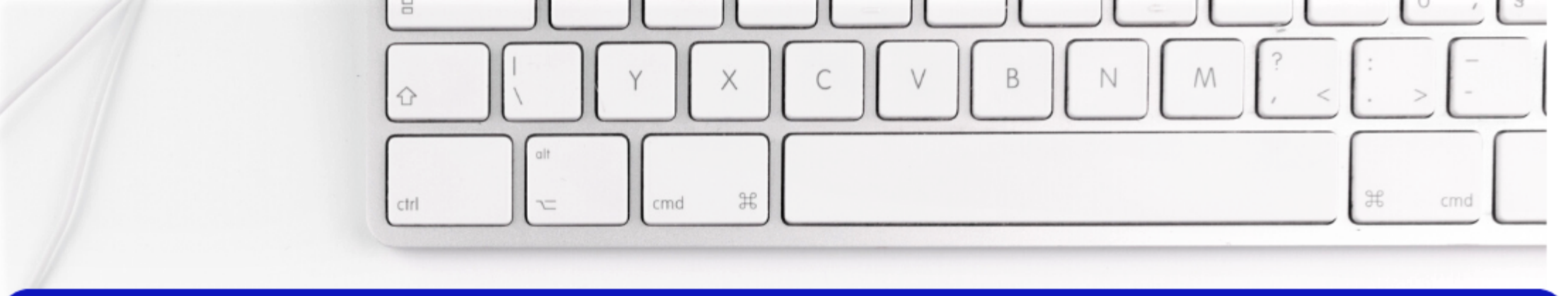
- Ensuring that websites use only HTTPS and do not provide HTTP versions; and installing browser plugins, at users' ends, to enforce the use of HTTPS only.
- Using public key pair-based authentication, like RSA, to ensure the authenticity of communication.

Follow us

Visit

Hackercombat.com

SWIPE



Hacker Combat Partnership

- Social Media Campaigns
- Sponsored Video
- Sponsored Article
- Sponsored Infographic
- Sponsored Multimedia Piece
- Banner Ads In Our Website
- Promotion Via Our Website

Increase brand awareness and drive revenue through **content sponsorship**

Contact us at:

Partners@hackercombat.com

Follow us

Hackercombat.com