Case Study: Web Jacking

1. Executive Summary

This case study explores how In 2015, the website of Domino's Pizza India was hacked, and sensitive customer information was stolen, causing reputational and financial loss.

2. Details about the attack.

- Data related to over 18 Cr orders from pizza chain Domino’s India appeared on the dark web.
- 13TB of employee files & customer details, which allegedly belongs to @dominos_india have been leaked on the Dark Web through a search portal that gives access to sensitive info of the users.
- The database includes personal details of the customers provided to Domino’s India when they placed an order through its website or app. These include names, phone numbers, email IDs, addresses and payment card details
- The database was being sold on the dark web for around two to eight bitcoins, with a **50 bitcoin** ransom for the company to block the sale of its data.
- the data stolen from Domino’s India’s database is from the period between 2015-21
- The company did not respond to questions about the severity of the customer location and phone numbers data being leaked.

Web Jacking:

Web Jacking is a cyber-attack where attackers create a fake version of a legitimate website to trick users into entering their credentials or sensitive information.

Methods used in Web Jacking:

- Domain Spoofing – Attackers register similar domain names to mislead users (e.g., "g00gle.com" instead of "google.com").
- Cross-Site Scripting (XSS) – Injecting malicious scripts into a trusted website.
- DNS Hijacking – Manipulating DNS records to redirect traffic to a malicious website.
- Phishing & Social Engineering – Fake login pages that steal user credentials.

Countermeasures for Website Security:

Use HTTPS & SSL Certificates – Encrypt communications to prevent data interception.

Enable DNS Security Extensions (DNSSEC) – Prevent DNS hijacking.

Regularly Monitor & Audit Websites – Detect unauthorized changes early.

Implement Multi-Factor Authentication (MFA) – Reduce the risk of stolen credentials.

Educate Users on Phishing Risks – Prevent social engineering attacks.

Case Study: Password Sniffing on a Public Wi-Fi Network

1. Incident Overview

A group of attackers used a password-sniffing tool on a public Wi-Fi network to intercept users' login credentials. The attack exploited unencrypted communications, allowing hackers to capture usernames and passwords in real time. Victims included online banking users, social media account holders, and employees accessing corporate emails.

2. Risks of Using Unsecured Networks

- Man-in-the-Middle (MITM) Attacks – Attackers intercept data between users and websites.
- Session Hijacking – Unauthorized access to user sessions after login.
- Packet Sniffing – Tools like Wireshark capture unencrypted data packets.
- Data Theft & Credential Leaks – Sensitive information is stolen and misused.

3. Countermeasures for Website Security

- Use HTTPS Websites – Encrypts data, preventing sniffing.
- Enable VPN – Encrypts internet traffic on public networks.
- Use Multi-Factor Authentication (MFA) – Adds an extra layer of security.
- Avoid Public Wi-Fi for Sensitive Transactions – Use mobile data instead.
- Use Strong, Unique Passwords – Prevents attackers from reusing stolen credentials.
- Monitor Login Activity – Detect unauthorized access attempts.