Security Incident Report

Step 1: Access the Template

Step 2: Identify the Network Protocol

- Protocol Identified: The primary network protocols involved in this incident include:

  - DNS (Domain Name System): Used for resolving the URL yummyrecipesforme.com to its corresponding IP address.

  - HTTP (Hypertext Transfer Protocol): Used for the requests made by the browser to load the website and download the executable file.

Step 3: Document the Incident

- Summary of the Incident:

On 23rd September, 2024 , the website yummyrecipesforme.com experienced a security breach due to a brute force attack executed by a former employee. The attacker utilized default passwords to gain unauthorized access to the web host's administrative panel. Upon successful login, the attacker modified the website's source code by embedding a malicious JavaScript function that prompted users to download an executable file. This file contained malware and redirected users to a fake site, greatrecipesforme.com, which led to compromised user devices.

The incident was discovered when multiple customers reported receiving prompts to download a file for free recipes. Upon further investigation by the cybersecurity team, it was confirmed that the attacker had changed the administrative password post-attack, preventing the website owner from regaining access.

The logs indicated a DNS request initiated by the browser to resolve the IP address for yummyrecipesforme.com, followed by an HTTP request to download the malware. This was succeeded by further DNS and HTTP requests leading to greatrecipesforme.com.

Sources of Information:

- Customer emails to the helpdesk

- Network protocol analysis using tcpdump

- Source code examination by the senior analyst

Step 4: Recommend Remediation for Brute Force Attacks

- Recommendation: Enforce Strong Password Policies

Implementing strong password policies is an effective measure to prevent brute force attacks. Strong passwords should contain a mix of upper and lower case letters, numbers, and special characters, and should be of a significant length (e.g., at least 12 characters). This complexity makes it significantly harder for attackers to successfully guess passwords within a reasonable timeframe.

Additionally, the organization should implement password change requirements and monitor login attempts to identify and respond to suspicious activity. This will help reduce the risk of unauthorized access and protect sensitive user data.