Security incident report

Section 1: Identify the network protocol involved in the incident

The network protocols involved in this incident are:

1. DNS (Domain Name System): The browser initially requested a DNS resolution for the "yummyrecipesforme.com" URL, which is a fundamental step in converting the human-readable domain name into an IP address.
2. HTTP (Hypertext Transfer Protocol): After obtaining the correct IP address through DNS, the browser initiated an HTTP request to the "yummyrecipesforme.com" webpage, which is the standard protocol for retrieving web content.
3. File Download: The browser then initiated the download of an executable file, which was prompted by the compromised website. The specific protocol for file download may depend on the file type, but it commonly involves HTTP or FTP (File Transfer Protocol).
4. DNS (Again): Following the download of the executable file, the browser requested another DNS resolution, this time for the "greatrecipesforme.com" domain. This step was crucial for redirecting users to the fake website.
5. HTTP (Again): With the new IP address obtained from the DNS resolution, the browser initiated another HTTP request, this time to the new IP address associated with "greatrecipesforme.com.

Section 2: Document the incident

The incident involved a security breach of the "yummyrecipesforme.com" website, resulting in the following sequence of events:

1. Unauthorized Access: An attacker gained unauthorized access to the website's admin panel by performing a brute force attack. The attacker repeatedly attempted to log in using known default passwords until they successfully guessed the correct one.
2. Code Modification: Once inside the admin panel, the attacker modified the website's source code. They embedded a malicious JavaScript function that prompted visitors to download and run an executable file when accessing the website.
3. File Download and Redirection: Visitors who downloaded and ran the file were subsequently redirected to a fraudulent website, "greatrecipesforme.com," which

mimicked the original site's appearance. On this fake website, the company's recipes were made available for free.

4. DNS Resolutions: The DNS was used multiple times in this incident. Initially, it resolved the IP address for "yummyrecipesforme.com," allowing the attacker to access the legitimate site. Later, it resolved the IP address for "greatrecipesforme.com," redirecting users to the fraudulent site.

Section 3: Recommend one remediation for brute force attacks

To prevent future brute force attacks and enhance the security of the website, the following remediation steps should be taken:

1. Implement Account Lockout Policy: Set up an account lockout policy that temporarily locks an account after a certain number of failed login attempts. This would deter attackers from repeatedly trying different passwords. After a specified time period or manual intervention by an administrator, the account can be unlocked.
2. Enforce Strong Password Policies: Ensure that all administrative accounts have strong and unique passwords. Passwords should be a combination of letters, numbers, and special characters, and they should be changed regularly. Default passwords should be disabled or changed immediately upon installation.
3. Implement CAPTCHA or Rate Limiting: Implement CAPTCHA challenges or rate limiting on login attempts to make it more challenging for automated brute force attacks. This would require human interaction to prove that the login attempts are legitimate.
4. Monitor and Log Failed Login Attempts: Continuously monitor and log failed login attempts. Suspicious login patterns should trigger alerts to the cybersecurity team for immediate investigation.
5. Regular Security Audits: Conduct regular security audits and vulnerability assessments to identify and address any potential weaknesses in the website's security posture.
6. Educate Administrators: Train administrators on best practices for securing their accounts and recognizing phishing attempts. Social engineering attacks, such as phishing, can also lead to compromised passwords.

By implementing these security measures, we can significantly reduce the risk of future brute force attacks and enhance overall cybersecurity.

Luca Forma