Security incident report

CASE STUDY-02
Incident Response: Brute Force & Malware Injection – *yummyrecipesforme.com*
Investigated a security breach where a former employee executed a brute force attack to access admin credentials. Identified malicious JavaScript code embedded in the site to deploy a malware-laced download that redirected users to a spoofed domain. Used tools like tcpdump and sandboxing to analyze DNS/HTTP behavior.
Key actions: Identified weak credential practices, confirmed JS-based redirection malware, and recommended account lockout policies and strong password enforcement to prevent future brute force attacks.

Incident ID: 2025-05-002
Date/Time Reported: 2025-05-12, 10:30 AM
Reported By: Navya Nagpal, Cybersecurity Analyst
Department: IT Security

After several hours of attack, the website owner informed the website hosting provider about multiple complaints from the website's helpdesk regarding the slowdown of their personal systems.

Section 1: Identify the network protocol involved in the incident
The network protocol involved in this incident was the Domain Name System (DNS) &

Hypertext Transfer Protocol (HTTP).
The DNS is used when the browser requests the IP for yummyrecipesforme.com and later for greatrecipesforme.com. The HTTP was involved as the problem was with accessing the web server for yummyrecipesforme.com, as HTTP is used to serve the website content and a malicious file (in this case), forming the core of the exploit. The requests to web servers for accessing the website and its pages involve HTTP traffic.

Section 2: Document the incident

A brute force attack was executed to gain access to the web host of the website, namely, yummyrecipesforme.com. The attacker leveraged a dictionary-based brute force method, where the attacker uses a precompiled list of likely passwords. After guessing the right credentials, they embedded a JavaScript function in the source code that redirected visitors to the fake version of the website, namely greatrecipesforme.com. The malware that made customers download the malicious file. Upon running that infected file, the customers' personal computers began running more slowly. Upon receiving the complaints on the website's helpdesk, the website owner tried logging in to the admin panel and failed to do so.

The cybersecurity analysts created a sandbox environment to observe the website's suspicious behaviour. When they ran the website on the network analyzer tcpdump, they observed that the browser redirects them to a different URL, which delivered the malware. A senior analyst confirmed the attack that compromised the website.

The cause of the attack, as analyzed by the team of cybersecurity, was not updating the passwords timely as the admin password was found to be set as default, which allowed the hacker to guess it through the 'dictionary' of the previous frequently possible passwords. Also, it was observed that there were no safety and preventive measures to prevent a brute force attack.

Section 3: Recommend one remediation for brute force attacks

One preventive measure that the team advised to prevent future brute force attacks is the updation of passwords so that it is not an easy task for the malicious actors to access them. Using previously used passwords allows hackers to brute force the system or the network by checking the dictionaries and lists they've made from the previous breaches. A strong & unique password must be set and changed regularly to

prevent such breaches.

Actions taken:

1. The website was taken down temporarily.
2. Regaining and resetting the Admin Credential
3. Securing the Admin Credentials
4. The malicious code was removed from the website
5. Scanning for any other backdoors
6. Informing the affected users about the attack and providing them measures to resolve the issue.

Reported by:
Navya Nagpal
IT Security Analyst
Signature: _____
Date: 2025-05-20