# Security incident report

Scenario:

In this incident, this shows an issue where a website got hacked and it was replaced with a fake website. This website “yummyrecipesfor.com” was compromised by a malicious cyber-attacker to exploit the security vulnerabilities and utilize any means to attack the security framework to take advantage of anything necessary for criminal means. This documentation shows the steps taken to combat against the issue.

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The network protocol that got involved in this incident with the Hypertext transfer protocol server along with the IP address being compromised during this incident. There was a website that got hacked and was replaced with a fake website. A tcpdump was run to detect any issues. As I was accessing the yummyrecipesforme.com website to detect the problem, capture protocol, and traffic activity in a DNS & HTTP traffic log file provided the evidence needed to come to this conclusion. The malicious file was observed being transported to the users’ computers using the  HTTP protocol at the application layer.  . |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Several customers contacted the website owner stating that when they visited  the website, they were prompted to download and run a file that asked them  to update their browsers. Their personal computers have been operating  slowly ever since. The website owner tried logging into the web server but  noticed they were locked out of their account. This caused a massive red flag to be investigated. The cybersecurity analyst used a sandbox environment to test the website without impacting the company network. Then, the analyst ran tcpdump to capture the network and protocol traffic packets produced by interacting with the website. The analyst was prompted to download a file claiming it would update the user’s browser, accepted the download and ran it. The browser then redirected the analyst to a fake website (greatrecipesforme.com) that looked identical to the original site (yummyrecipesforme.com). The cybersecurity analyst inspected the tcpdump log and observed that the browser initially requested the IP address for the yummyrecipesforme.com website. Once the connection with the website was established over the HTTP protocol, the analyst recalled downloading and executing the file. The logs showed a sudden change in network traffic as the browser requested a new IP  resolution for the greatrecipesforme.com URL. The network traffic was then  rerouted to the new IP address for the greatrecipesforme.com website.  The senior cybersecurity professional analyzed the source code for the  websites and the downloaded file. The analyst discovered that an attacker had  manipulated the website to add code that prompted the users to download a  malicious file disguised as a browser update. Since the website owner stated  that they had been locked out of their administrator account, the team  believes the attacker used a brute force attack to access the account and  change the admin password. The execution of the malicious file compromised  the end users’ computers. At 2:18pm the website yummyrecipes was trying to establish a connection with the DNS domain address to connect the site for users to log in. Leading into 2:20pm to 2:25pm that domain site DNS got compromised with its address being switched to “greatrecipesforme.com”. The hacker decided to use a bruteforce attack to infiltrate the site’s security functions and then redirect the DNS domain to the IP address to a different site to abuse the functions of it and hack other users that will click on the site to be compromised with more infected base resources done by the hackers. The site is vulnerable at the point when it redirects you to a different site and therefore the hacker collects the data from users entering to perform the threats it plans to do to harm any victim's identity/etc. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| I would recommend using a heavily defended firewall with strict security policies where certain authorized users can access information on the website to better protect its functions. Also, I would enable 2 factor authentication along with heavy strong password management software where it’s randomized to protect people’s data. I would suggest adding a one time password verification method to enforce stronger security framework defenses. This way it goes after the hacker when it’s compromised on their end to be detected the minute they try to perform another attack. I would also, recommend installing strong anti-malware software to detect any potential activity from hackers on top of implementing a strong intrusion detection system on top of an intrusion protection system to defend all incoming network traffic and system vulnerability/exploit activity done by potential hacking threats. |