# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| From the logs obtained from tcpdump, we can see that the HTTP protocol was used to connect to the site. The DNS redirection leads the user to a spoof site and forces the user to make a HTTP/GET request possibly making them download a malicious file. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| IT team is being informed several hours after the attack by multiple customers. Customers complained about company’s website prompting them to download a file to access free recipes, after running the file, the address of the website was changed and their computers began running more slowly. The owner of the website tried to log in to the admin panel but was unable to.  To observe the suspicious website behavior, we created a sandbox environment and ran the network protocol analyzer tcpdump. After that, we tried to connect to the website “yummyrecipiesforme.com” and as soon as the website loads, the site requested to download and execute a file to update the browser and let us view the free recipes.  After analyzing the logs, it was found that the request made for yummyrecipesforme.com reaches DNS server and DNS replies with the correct IP address. The browser initiates HTTP request for the site using the IP address sent by DNS. After that browser initiates the download of the malware. Then the browser initiates a DNS request for “greatrecipesforme.com” which is the spoof site. After the response of DNS the browser initiates the HTTP request to the IP address of the site.  A senior analyst confirmed that the website was compromised. After checking the code, they found that a javascript code was added to prompt the visitors to download an executable file. Analysis of this file exposed that there is a script that redirects the visitors’ browsers from “yummyrecipesforme.com” to “greatrecipesforme.com”.  The cybersecurity team reported that web server was impacted by a brute force attack. The hacker was able to admin password because it was set to the default password, and there were no additional controls to prevent brute force attack. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| The first and most important step to harden the security is to change the default set admin password to a complex password and if the admin interface is not being used too frequently, an extremely hard password can be set and secured physically to prevent anyone from accessing.  Another additional step that can be added to make the hackers job harder is changing the password in certain time periods, may be once in four months.  Also, an additional MFA (multi factor authentication) for the admin access can prevent the unauthorized people from accessing the admin interface just by knowing username and password.  Another common addition that can be done is wrong password counter. This can count the number of wrong passwords and if anyone tries to log in with a wrong password for four times, their account can be locked. This is one of the most common technique to prevent brute force attacks, since the attacks depend on try & fail until the password is true technique and the method blocks multiple wrong inputs.  An another addition that can be done to also detect the malicious actor is IP/Location detection. By adding a notification that contains the IP and location of the person that either logs in or attempts to log in, the authorized person can be informed about both the attempts and the person that is attempting to break in. |