# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The network protocol involved in the incident is Hypertext Transfer protocol (HTTP)at the application layer. Running network protocol analyzer (tcpdump) and assessing the organization's website which is the yummyrecipesforme.com. When the browser initiates HTTP request to the webpage, it then after downloads the malicious file which customers are redirected to fake webpage, designed to look like the original site. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| Several customers emailed yummyrecipesforme.com’s helpdesk stating that the organization’s website had prompted them to download a file to update their browser. Customers claimed that, after running the file, the address of the website changed and their personal computer began running slowly. In response to this incident, the website owner tried to login to the admin panel but was unable to and reached out to the website hosting provider.    The cybersecurity analyst created a sandbox environment to observe the suspicious website behavior. Then the analyst ran the tcpdump to capture network and traffic packets produced by interacting with the website. The analyst was prompted to download a malicious file, same with what the customer is experiencing. The analyst then runs the file and observes as it redirects to another website, greatrecipesforme.com, which is designed to look like the original one which is the company’s website, yummyrecipesforme.com  The cybersecurity analyst inspected the tcpdump log and observed that the browser initially requested the IP address for the yummyrecipesforme.com. Once the connection is established over the HTTP, with the malicious file that was executed earlier. The logs then suddenly change in network traffic as the browser requests new DNS resolution for the greatrecipesforme.com URL. The network traffic was then rerouted to the new IP address which is the greatrecipesforme.com website.  The senior cybersecurity analyst confirms that the website was compromised. He checked the source code for the website and noticed that a javascript code had been added to the prompt website visitor to download an executable file. The cybersecurity team reports that the web server was impacted by a brute force attack to access the account and then changed the admin password. The execution of the malicious file compromised the customer’s computers. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| The team plans for two security measures to be implemented to protect against brute force attack.One, having two-factor authentication (2FA). This 2FA plan is an additional requirement for users to verify their identity in two or more ways to access the system or network. Two, requiring strong passwords. Passwords that follow specific rules like a minimum of 8 characters, a capital letter,number, and a symbol rather than a default password. Through this, malicious actors will not likely to gain access to a network or system through a layer of network/system security. |