# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| The protocol impacted in the incident is Hypertext transfer protocol (HTTP).  Running tcpdump and 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 is 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.  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. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| Recommendation to avoid brute force attacks is to implement password policy to require length and type of characters allowed and disallowed and could also disallow an entry for a dictionary of unwanted terms.  To make sure all employees are compliant and follow the minimum requirements, I would recommend a centralized password management system that enforces the password policy and also consider enforcing two-factor authentication (2FA) on all admin accounts.  Make sure not to use default admin credentials and make sure they are updated and also for policy for this to be updated on time schedule and when recent admins leave. |