# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The protocol involved with this incident relates to the web server and due to the ability for the hacker to change the source code means that the security mechanisms were poor. This leads us to the HTTP protocol involving traffic for less secure web servers. Additionally, the malicious file request initiates itself as a HTTP request for the manipulated source code. |
|

|  |
| --- |
| **Section 2: Document the incident** |
| This event occurred when numerous customers contacted the site’s helpdesk claiming that upon visiting the site they were prompted to download and run an executable file to gain access to the content. The owner subsequently attempted to login to the web server and noticed they were locked out of their admin panel.  Cybersecurity professionals then attempted to examine the issue in a sandbox environment to limit any issues. A tcpdump program was utilized for packet capture and analysis, which led to the prompt of a file for downloading and executing. This process redirected the analysts away to the malicious site.  A senior analyst discovered that the attacker had manipulated the site to change code that added the file into a downloadable file disguised in the browser. The analysts concluded that since the owner was locked out of his account that a brute force attack was implemented to access and change the account details. This led to the execution of a malicious file compromising the end user’s computers. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| One recommendation would be to change the login credentials of the owner’s account. It is important for the owner to understand that default credentials should always be changed because it leaves networks vulnerable and it is very easy to mitigate by customizing the account details. Additionally, adding frequent password changes would help build resilience to an attacker that may have guessed a previous password. Furthermore, the use of two-factor authentication and one-time passcodes could make it even more difficult for an attacker to gain access to the account as this is a great way to specifically prevent brute force attacks from working in the future. |