Security incident report

Section 1: Identify the network protocol involved in the incident
Since the incident was a hacked website the evidence suggests that HTTP protocol was used. Based on the tcpdump traffic logs once the source computer starts connecting with yummyrecipesforme.com it is through the HTTP port (port 80). This also happens when connected to the spoofed website greatrecipesforme.com. The malware also uses an HTTP GET method to start the attack.

Section 2: Document the incident
A disgruntled ex-employee of yummyrecipesforme.com wanted to lure users to a spoofed website with malware as revenge. The ex-employee executed a brute force attack by using several known passwords to gain access to the administrative side of the website and change the password. Then add a javascript function that prompts visitors to download and run a file upon visiting the website. Once the file is downloaded it redirects the user to a spoofed website, greatrecipesforme.com, which contains malware. Seven hours after the users' visit their computers start to run slower. The website owner contacted the host company after being denied access to the website's administrative account. We created a sandbox environment to investigate the website further with a network protocol analyzer tcpdump. In the tcpdump, we observe that the code manipulates the HTTP protocol, once the malware file was running it ran an HTTP connection to the malicious website. Once the hack was confirmed we deleted the javascript function code and gave back ownership.

Section 3: Recommend one remediation for brute force attacks
I recommend that the website owner add a separation of administrative controls of the website like owner and employee accounts because there was none in place. I recommend the owner add an encryption key to all passwords

to prevent other employees from repeating this attack.