Security incident report

Section 1: Identify the network protocol involved in the incident
The main protocol that was involved in the incident was HyperText Transfer Protocol (HTTP). HTTP is the protocol that is used for requesting and delivering webpages between the web server and the user device. This is seen through the tcpdump log files that show that HTTP was used to initially connect to yummyrecepiesforme.com, download the malicious file, and then connect the user to the spoofed greatrecepiesforme.com

Section 2: Document the incident
The effects of the incident were first noticed by users of yummyrecepiesforme.com who reported to the client that they were prompted to download a file from the website, and were then redirected to greatrecepiesforme.com when said file was run. The website owner attempted to log into the administrative panel for yummyrecepiesforme.com, but was not allowed access to the administrative controls. This is then where the security team was brought into the incident. The team retraced the reported steps of the users in a secure sandbox environment while running the network analysis tool “tcpdump.” The same prompt to download a file and redirection to greatrecepiesforme.com after execution of the file occurred upon connection to yummyrecepiesforme.com in the sandbox environment. Inspection of the logs that were gathered by the network analysis tool showed that after a query to a DNS server for the IP address of the original website and a HTTP connection was made with the web server, web traffic was redirected to the spoofed website. The team notes that they downloaded and ran the prompted file before they were redirected to the spoofed website. A senior analyst inspected the source code of the websites and malicious file and found that the original website was tampered with and had code injected into that was responsible for prompting the user to run the malicious file that disguised itself as a requirement to access recipes.

With the original website owner being unable to access their account, the team believes that the malicious actor was able to brute force their way into accessing the administrator account on the website, where they then injected their malicious code and changed the password to the administrator account so that it could not be logged into by anyone else.

Section 3: Recommend one remediation for brute force attacks
The team suggests strengthening password policies to help prevent against the administrative password being guessed using brute force tactics again. Using any sort of default passwords or rotation of passwords is also not recommended. Furthermore, if a password was used in the past, it should not be allowed to be used again. Passwords should ideally be original, contain a mixture of letters (lower and upper cases), numbers, and symbols, and not shared between any accounts. Furthermore, some sort of two-step/two-factor authentication should be used. This places another lock onto the account in the event that the password is learned. It would be extremely difficult for malicious actors to gain access to the administrative controls of the website without gaining access to some other account for mobile numbers if two-step were to be used.