# Security incident report

| **Section 1: Identify the network protocol involved in the incident** | |
| --- | --- |
| This incident was analyzed using a protocol analyzer TCPdump, The DNS & HTTP traffic log showed a field request “HTTP: GET / HTTP/1.1” was made, which could indicate the download of a malware. The protocol impacted in the incident is Hypertext transfer protocol (HTTP). After the request a new TCP handshake was initiated which redirects website visitors to another website “greatrecipesforme.com.”. This website redirection is likely the result of malware. | |
|

| **Section 2: Document the incident** |
| --- |
| This incident was reported by yummyrecipesforme.com visitors about a prompt for a file download for users to update their browser. After the file was downloaded they noticed a slow down in their devices operating speed.It was reported to the security team when the website owner was unable to access their website.  The cybersecurity analyst proceeded to visit the yummyrecipesforme.com website to run a network protocol analysis using TCPdump in a sandbox environment, as to avoid infecting the network in a chance that is a malware attack. .  Similar to website visitors, the cybersecurity analyst was prompted to download a browser file update once the connection with the website was established over the HTTP protocol, which they did. The tcpdump log showed a change in network traffic as the browser requested a new IP resolution for the greatrecipesforme.com URL, which initiated a website redirection. The redirection prompted a new TCP handshake process between the cybersecurity analyst device and greatrecipesforme.com.http with an IP address 192.0.2.17  It was confirmed by a senior cybersecurity analyst that the website's source code was modified to request the browser update file download, which contained a script that redirects the visitors’ browsers from yummyrecipesforme.com to greatrecipesforme.com. Also since the website owner stated that they were 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 initial report of device slow cause by the website visitor who downloaded the file was the malicious file compromising their devices. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| A brute force attack was used to gain access to the website admin account, which was using its default password, this gave access to the threat actor to modify the website source code. A two factor authorization involving a OTP (one-time password) being sent to the owners chosen device should be implemented to mitigate any further attempts of a brute force attack. |