**Nicholas Coleman**

# Security incident report

| **Section 1: Identify the network protocol involved in the incident** |
| --- |
| The protocol involved in this security incident is HTTP, which is evident from the logs. The logs show that the DNS protocol was successful in connecting the source computer to the client's website, so DNS is not the issue here. |

| **Section 2: Document the incident** |
| --- |
| We ran a sandbox environment to find out the cause of the issue that the client is facing. The source computer that is used, requests the client's website, and DNS directs them to the legitimate page. However, our findings revealed that a malicious actor has implemented their own code on the site, as it automatically redirects the source computer to a malicious site with a similar name to yummyrecipes.com. The log entry with the code: "HTTP: GET /HTTP/1.1", is most likely the cause of the issue: the download request for the malicious file that redirects the source computer. This is most likely the case because immediately after the abnormal HTTP request, traffic is routed from the source computer to the DNS server again, using port .52444, to make a new DNS resolution request, which leads to the malicious website itself. |

| **Section 3: Recommend one remediation for brute force attacks** |
| --- |
| The most likely cause of this attack was due to insecure password practice at the client company. A malicious actor was able to brute force their way into the website using the admin username and password. To prevent this attack from being possible in the future, the client should implement Multi-Factor Authentication/Two-Factor Authentication on their websites. This will protect the websites from brute force attacks, as the attacker must have more than just a username and password. |