# Security incident report

|  |
| --- |
| **Section 1: Identify the network protocol involved in the incident** |
| The network protocol involved in the incident is the Hypertext Transfer Protocol. Shown by Port 80 being involved as well as the log entry of HTTP: GET / HTTP/1.1 |
|

|  |
| --- |
| **Section 2: Document the incident** |
| The IT Department started investigating the incident by using a sandbox environment. By using a Network Protocol analyzer tcpdump and running the website URL in the sandbox we found that there was a source computer (your.machine.36086) sending a connection request to Port 36086. The communication between the source and the intended  destination Port 36086 continues for about 2 minutes. After such the log entry shows the code HTTP: GET / HTTP/1.1 which could indicate the request to download malicious file software. After that log there is noticeable change: the DNS server is shown again routing to the source computer using port .52444 to make another DNS resolution request. This time rerouting the DNS traffic to a new IP address. (192.0.2.172) and its associated URL (greatrecipesforme.com.http). Making traffic reroute to the source computer and spoofed website URL. The source computer is shown changing its Port number to (.56378) when the traffic rerouted to the Spoofed website. |

|  |
| --- |
| **Section 3: Recommend one remediation for brute force attacks** |
| The IT department believes the best course of action is requiring and enforcing two-factor authentication (2FA). With 2FA every login will be protected from brute force login attempts, by requiring two ways to authenticate the user identity when failing to log in the first time. While requiring stricter password policies would also help, 2FA will go a step further to avoid dictionary brute force attacks and malicious threats attempting to guess an employer/employees password. |