Security incident report

Section 1: Identify the network protocol involved in the incident
HTTP is the network protocol that isn involved in this incident. This can be seem using the tcpdump application it is seem that HTTP is used to send the corrupted file to the customers' computers.

Section 2: Document the incident
Customers contacted the manager to indicate that the website had suspicious activity (forced download and slowing of machines). This was then investigated by cybersecurity engineers who recreated the scenario on a sandbox computer. They were able to understand the network protocol involved and the reason why the computers were slowing down. Due to this, they could then offer remediations to prevent an incident like this to occur again.

Section 3: Recommend one remediation for brute force attacks
Since this was a brute force attack, one remediation would be enhanced password setting. It would be much safer to have a certain criteria of password regulations (certain characters, special symbol, numbers and letters). This will severely lower the number of brute force attacks that work.