Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocol involved is the HTTP protocol.

Section 2: Document the incident
After there were a few customers reporting an anomaly in the behaviour of the website, a group of cybersecurity analysts decided to address the incident and try to observe the website inside a sandbox environment. The team discovered that the logs showed an abnormal DNS request in the 14:20:32 log, where the client requested, with the port 56378, the IP address of the greatrecipesforme.com website. Then, the client sets a connection with the server after the corresponding ACK/SYN handshake and, GET request to the server, where the team assumes the malware is downloaded.

Section 3: Recommend one remediation for brute force attacks
A good way of preventing these sorts of attacks could be, to monitor the logs and set an alarm for suspicious activity so, when a suspicious IP is recognized to be trying to access the server via a brute force attack, the team can block the IP address. However, a more long-term solution can be the implementation of MFA, to prevent malicious actors to just getting a new IP with any form of IP spoofing and re-try the attack.