

Team 1

LEGP21A

To the Business Management team:

I am writing to report on the recent DOS attack on the network. The objective of this memo is to help explain what happened and what can be done in the future to prevent such availability outages from reoccurring.

At 3:32 PM on Tuesday, the website team began noticing a noticeable slowdown in responsiveness to people trying to view the website and view our products. Ten minutes later, the entire website began to shut down due to an unnatural number of people attempting to access the site. When the website team noticed this, they contacted the information team, who then realized that almost all of these connection attempts were from Kazakhstan, which is not an expected customer of our products. They realized that they were being attacked by a DDOS attack, meaning that a large number of infected PCs were trying to use up all our computer power in order to deny access to legitimate customers.

After adapting our firewall settings to block all traffic from Kazakhstan, the attack relented. However, this is not a permanent solution, as there may be some legitimate customers. In the future, it is the recommendation of the Information Technology team that we invest in partnering with a cloud service provider such as CloudFlare in order to protect against DDOS attacks.

If you have any questions or need further information, please do not hesitate to reach out.

Best regards,

Group 1