Security incident report

Section 1: Identify the network protocol involved in the incident
The network protocol involved in this incident occurred at the HTTP level. Because the reports came from accessing the yummyrecipesforme.com website, the requests to web servers are through HTTP protocol. Furthermore, the tcpdump logs indicate that requests were made at the HTTP level at the application layer of the TCP/IP model.

Section 2: Document the incident
The following is the incident reported in a sandbox environment after multiple complaints of an irregular file download appearing when first entering the website. This download offered free recipes and took users to a different URL and locked them out of their accounts. They reported slow computer computations after this incident. The following is a tcpdump log analysis summary of what occurred in the sandbox environment. - At 2:18pm a request is sent from “your machine” to the yummyrecipesforme.com website using port 52444 to the Google DNS to obtain the IP for the said website. - This is followed by an IP address from the Google DNS. - Using that IP address, “your machine” requests a “connection start” to the yummyrecipesforme.com website with its appropriate IP address - This request is followed by a “connection start” acknowledgement from the yummyforme.com website. - “Your machine” sends an acknowledgement message to the website. - Then “your machine” sends a “data push” acknowledgement with the following request: HTTP: GET / HTTP/1.1 - The yummyrecipesforme.com website acknowledges this request - Time passes with much information through port 80 - At 2:20pm, another request to Google DNS is sent from “your machine” to a different website - greatrecipesforme.com website - The IP address is received and “your machine” requests a “connection

start" to greatrecipesforme.com
- This connection is acknowledged both ways and then another HTTP: GET / HTTP/1.1 request occurs

It appears that the attacker used an old password to login and change the source code on the website, thereby allowing a malware download in the form of a free recipes link that redirects them to a fake website and locks them out of their accounts.

Section 3: Recommend one remediation for brute force attacks
One recommendation that may help prevent an attack from this type of malicious brute force attack would be to update/change passwords at regular intervals and/or ensuring that those in a role with significant access to controls or information have immediately expired passwords once an employee is no longer with the company.