Security incident report

Section 1: Identify the network protocol involved in the incident

The network protocol used is HTTP which is visible because of the TCPDump where you can see to interact with the malware HTTP is used as well as is carried by HTTP protocol onto Users computer.

Section 2: Document the incident

Users contacted management to alert of problems with a redirect to a fake website after a link prompt to get “Free material” of our paid recipes and books sent users to the false duplicate website that would have the malware installed and caused their devices to become slow.

Owner of the website tried to log in but was unable to due to a password being changed which we believe was cracked using brute force. We then were contacted to help and investigate the attack.

We used a Sandbox to contain the malware and observer it which found that the malware was implemented in order to redirect users in the websites source code using javascript to make a query from normal website to false website with malware

Must implement better password requirement policies for the company and MFA or more secure ways of authorization in order to keep website safe.

Section 3: Recommend one remediation for brute force attacks

Best one is Multi Factor Authorization which directly stops attackers due to needing a second verification which helps mitigate risk of attackers getting into accounts. Having users with administrative roles or roles with access to sensitive information be forced to use MFA which would keep systems safe. Along with adding rate limiting to access accounts it could stop consecutive brute force attacks.