Security incident report

Section 1: Identify the network protocol involved in the incident

HTTP is the protocol involved. The document that is being downloaded by clients is malicious and utilizes this protocol to slow down their computers and accessing the users' information. The tcpdump we conducted shows the same results that we are using an unsecure protocol and actors took this as an advantage to attack.

Section 2: Document the incident

The incident occurred was raised at the websites helpdesk that customers were prompted to download a file and view free recipes when they accessed the site. Customers also mentioned that the address of the website changed, and their computers slowed because of this.

The owner also attempted to access the site but was locked out.

The analyst proceeded to use a sandbox environment and ran a tcpdump so we could open and monitor the site network traffic by performing the same steps customers used to access and download the file. The site would redirect to a different address using a fake website. The logs was a truth book of these activities showing the initial call, downloading and the fake website over this HTTP protocol.

The senior analyst confirmed the compromise which proceeded to analyze the source code for the website. They noticed that the attacker added code to alert the users to download the file. This compromised customers where computers ran slow and owners account was compromised of the password. This attack was aimed to get access to the account which the owner was locked out of. This has been concluded that this is an act of brute force attack.

Section 3: Recommend one remediation for brute force attacks

To avoid this, we can make use of sandbox environments in Virtual Machines to check any suspected files. This way we can test for vulnerabilities, run simulations of past attacks that the site has faced. The VM box can run these vulnerabilities to address any bugs that might have been unnoticed. In this we can improve the password policies, reCAPTCHA, hashing etc.