Security incident report

Section 1: Identify the network protocol involved in the incident

The Network protocols involved in this incident were HTTP (Port 80) and DNS (Port 53). These protocols were maliciously used to redirect users to a different URL that contained Malware.

Section 2: Document the incident

First, we noticed multiple emails from customers about redirecting issues with the website and complaints of slowness after being directed to download a file. The website owner tried logging into the admin panel but was unable to, which made us think a malicous act was happening. So, the Cybersecurity analyst started running the “tcpdump” tool. We discovered that we were able to make a DNS & HTTP request and connection to yummyrecipesforme.com, with the IP address of “203.0.113.22”. I was able to see certain flags like “Flags [S]”, which told me the web server was responding to the HTTP & DNS request. But shortly after the log shows the code “HTTP: GET/ HTTP/1.1”, which means the browser is requesting data from the website, and we think that is the download request for the malicous file. Then we see a change happen in the logs, we see our pc (the one we are troubleshooting on) make another DNS resolution request, using a different port number (Port 5244), which was routed to the IP address “192.0.2.172”, with the URL “greatreci[esforme.com”. Then we see all traffic start routing to that website. This incident would be a part of the known “Brute Force” attack, which also led to a “Watering Hole” attack.

Section 3: Recommend one remediation for brute force attacks

We recommend that the website owner set a password policy on the admin account that limits the amount of password attempts before the account is locked. Also, use a more complex password and do not allow previous passwords to be used. The Owner should be changing the password more frequently in this policy as well, we suggest every 60 days. MFA (Multi-Factor Authentication) should be set up when accessing this account to add a layer of security, by providing another form of authentication (like a one time passcode) to access the account.