Cybersecurity Incident Report: Network Traffic Analysis

As part of the DNS protocol, the UDP protocol was used to contact the DNS server to retrieve the IP address for the domain name of yummyrecipesforme.com. The ICMP protocol was used to respond with an error message, indicating issues contacting the DNS server. The UDP message going from your browser to the DNS server is shown in the first two lines of every log event. The ICMP error response from the DNS server to your browser is displayed in the third and fourth lines of every log event with the error message, “udp port 53 unreachable.” Since port 53 is associated with DNS protocol traffic, we know this is an issue with the DNS server. Issues with performing the DNS protocol are further evident because the plus sign after the query identification number 35084 indicates flags with the UDP message and the “A?” symbol indicates flags with performing DNS protocol operations. Due to the ICMP error response message about port 53, it is highly likely that the DNS server is not responding. This assumption is further supported by the flags associated with the outgoing UDP message and domain name retrieval.

The time these incidents occurred is between 1:24 - 1:28pm. We became aware of the incident after recieveing reports from several customer clients they were not able to access the company site. The network security team responded and began running tests with the network protocol analyzer tool tcpdump. The resulting logs revealed that port 53, which is used by the DNS was not reachable. We are continuing to investigate the root cause of the issue to determine how we can restore secure access to the web portal. Our next steps include checking the firewall configuration to see if port 53 is blocked and contacting the system administrator for the web server to have them check the system for signs of an attack. The most likely issue is an attacker was attempting to redirect users to malicious websites, intercept sensitive information or launch DDoS attacks.