# Cybersecurity Incident Report: Network Traffic Analysis

|  |
| --- |
| Summary: |
| As Part of the DNS protocol, the UDP protocol was used to contact the DNS server. The requested domain “yummyrecipesforme.com” cannot be accessed. This is based on customer feedback as well as the resulting logs from our own network analysis, which shows that in response to the UDP DNS a-record request, the ICMP echo reply returned the error message: ICMP 203.0.113.2 udp port 53 unreachable. Port 53, noted in the error message, is used for DNS communication by sending and receiving DNS queries and responses. This may indicate a problem with the DNS server. It is possible that this is an indication of a malicious attack on the DNS server.  This event is being handled by security engineers after the cybersecurity team reported the issue to their direct supervisor. |
|

|  |
| --- |
| Explanation: |
| The cybersecurity team became aware of the incident from several customers of our clients reporting that they were not able to access the client company website www.yummyrecipesforme.com and saw the error “destination port unreachable” after waiting for the page to load. The time of incident replication for analysis is: 13:24:32.192571 (1:24 p.m., 32.192571 seconds) Customers could not confirm the exact time the incident took place on their end.  Actions taken by the cybersecurity team to investigate the incident started with an attempt to visit the website where the error message “destination port unreachable” was replicated. To troubleshoot the issue, the network analyzer tool, tcp dump, was activated and packet sniffing tests began while another attempt to load the webpage was made. During its proper function, the process of loading a web page starts with your browser sending a query to a DNS server via the UDP protocol. This is done to retrieve the IP address for the website's domain name; this is part of the DNS protocol. The browser then uses this IP address as the destination IP for sending an https request to the web server to display the web page. The resulting log file reveals that when a UDP packet is sent to the DNS server, an ICMP packets containing the error message: “UDP port 53 unreachable” is returned.  Port 53 is a port for the DNS service. The error message “UDP port 53 unreachable” indicates the UDP message requesting an IP address for the domain “www.yummyrecipesforme.com” did not go through to the DNS server because no service was listening on the receiving DNS port.  The cybersecurity team has indicated several possible reasons for this issue:   1. The DNS server may be misconfigured, disabled, or down. 2. A firewall or security policy might be blocking UDP port 53 traffic to the DNS server. 3. The DNS server could be overwhelmed by traffic, making it unavailable for legitimate queries; possibly a **Denial of Service (DoS) attack.**   Security engineers continue to investigate. Their next steps include verifying the DNS server's status, checking for signs of an attack, ensuring its properly configured and running, and checking any firewalls or network policies affecting port 53 traffic. |

TCP Dump log samples on next page:

13:24:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24) 13:24:36.098564 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable, length 254 13:26:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24) 13:27:15.934126 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable, length 320 13:28:32.192571 IP 192.51.100.15.52444 > 203.0.113.2.domain: 35084+ A? yummyrecipesforme.com. (24) 13:28:50.022967 IP 203.0.113.2 > 192.51.100.15: ICMP 203.0.113.2 udp port 53 unreachable, length 150