

Cybersecurity Incident Report:

Network Traffic Analysis

Part 1: Provide a summary of the problem found in the DNS and ICMP traffic log.

Network protocol analyser logs indicate that port 53 is unreachable when attempting to access the domain "yummyrecipesforme.com". This is based on the error message returned via ICMP echo when attempting to access the domain. Given that port 53 is typically used for DNS requests, this seems to indicate a problem with DNS configuration or a DoS attack against the DNS server.

Part 2: Explain your analysis of the data and provide at least one cause of the incident.

The incident was first discovered at approximately 13:24 local time. Prior to this, multiple customers had contacted the organisation and reported receiving a "port unreachable" error message when trying to access the "yummyreceipesforme.com" domain. Incident was initially confirmed via packet analysis using network protocol analyser tcpdump. Protocol analyser logs revealed that port 53 (used for DNS requests) was unreachable. The network security team is continuing to investigate to confirm the cause. Next steps include investigating the DNS server to confirm if there has been a malfunction or if it is the target of a denial of service (DoS) attack and taking steps to resolve the issue.