Informe sobre incidentes de ciberseguridad: Análisis de tráfico de red

Parte 1: Proporciona un resumen del problema encontrado en el registro de tráfico DNS e ICMP.
Multiples clientes informaron que no se puede establecer conexion con la pagina web de la empresa, el equipo de seguridad procede a verificar las notificaciones de los clientes y en efecto no era posible hacer una conexion con la pagina web y se observa el error al cargar la pagina, “udp port 53 unreachable” era el mensaje que mostraba luego de esperar un tiempo a que intente a hacer la conexion. Luego de ejecutar el tcpdump notifica que el protocolo UDP que preparo la resolucion de DNS no pudo llegar al servidor DNS y no pudo obtener la direccion IP. En conclusion el protocolo afectado resulta ser el UDP y el servicio DNS.

Parte 2: Explica tu análisis de los datos y proporciona una solución para implementar
Al obtener el error "udp port 53 unreachable" lo siguiente a realizar para tratar de solucionar este error sera lo siguiente: - Verificar conectividad - Revisar la configuración del servidor DNS - Comprobar el estado del servidor DNS: - Reiniciar el router y el equipo - Configurar un firewall o antivirus: - Actualizar controladores de red: - Contactar al proveedor de servicios de internet (ISP) Si el problema persiste podria tratarse de un ataque por lo tanto se recomienda: - Análisis de tráfico con herramientas avanzadas: el objetivo es ver el trafico de red - Análisis de registros y eventos - Investigación de posibles ataques DDoS - Implementación de controles de seguridad adicionales: aumentar la seguridad de firewalll y los IDS/IPS - Coordinación con otros equipos de TI: colaborar con otros sectores TI para mitigar la amenaza - Monitorización continua y respuesta a incidentes: monitorización continua de la red y responde rápidamente a cualquier incidente de seguridad