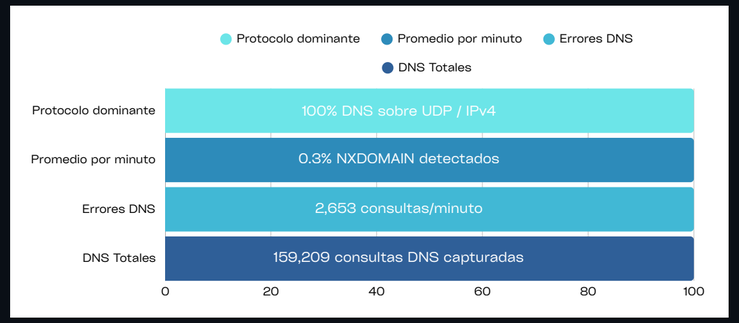
Informe de Análisis DNS en Entorno Virtual Aislado (Windows 10)

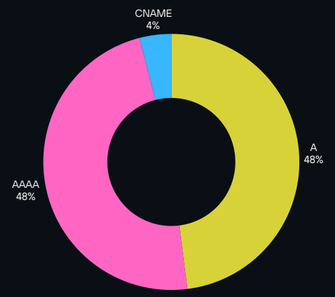
Por Jhailing Ramos – Analista en Ciberseguridad

Nov- 2025

Objetivo: Identificar el comportamiento del tráfico DNS generado por una máquina virtual Windows recién iniciada en entorno aislado, estableciendo métricas de volumen, patrones de consulta y detección de errores.

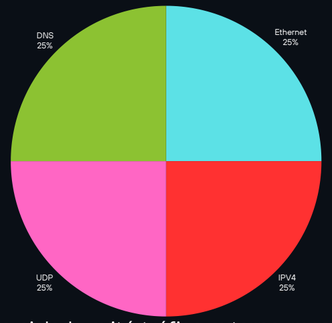


Distribución por tipo de consulta DNS



Windows usa resolución dual IPv4/IPv6

Protocolo por jerarquía



El entorno aislado evitó tráfico externo, mostrando únicamente protocolos de resolución DNS.

Conclusiones

- La VM generó un volumen intenso de consultas DNS iniciales causado por el arranque.
- No se detectaron indicadores de malware o comportamiento anómalo.
- El 0.3% de errores detectados (NXDOMAIN) fue analizado y se determinó que corresponden a pruebas controladas de resolución, descartando actividad de comando y control (C2) maliciosa.
- Entorno aislado ideal para análisis seguro.