Reporte de Inteligencia de Amenazas

8 de diciembre de 2025

Ibai Ruiz de Austri Lamas

1. Resumen Ejecutivo

El 8 de diciembre de 2025 a las 15:04 se ha producido una incidencia en la seguridad de la red, consistiendo esta del descubrimiento de un troyano vía HTTPS, este programa ha vulnerado el protocolo TLS y ha logrado infectar el equipo exitosamente. Esta brecha de seguridad puede suponer graves consecuencias como el filtrado de datos, la perdida de los mismos o la inutilización de los equipos en uso. Especialmente considerando lo rudimentario que era el malware empleado esto puede implicar que los sistemas de seguridad vigentes no están funcionando correctamente, de lo contrario este programa no podría haber infectado el equipo en primer lugar.

2. Contexto del incidente

Se ha analizado el tráfico registrado en el archivo decrypting_HTTPS_TLS_traffic.pcap empleando su respectivo archivo keylogger esto resulta necesario para poder desencriptar la información contenida en el tráfico HTTP registrado y así poder hacer un análisis en profundidad de la información transmitida.

3. Indicadores de compromiso

El archivo reconocido como malware, específicamente como un troyano, ha sido '*invest_20.dll*', proveniente del dominio '*foodsgoodforliver.com*' y con hash '*31cf42b2a7c5c558f44cfc67684cc344c17d4946d3a1e0b2cecb8eb58173cb2f*'.

4. Análisis e Inteligencia de Amenazas (TI)

Empleando la página web VirusTotal como herramienta de análisis se ha podido confirmar la naturaleza maligna del archivo tal y como se puede apreciar en la **Figura 1.**

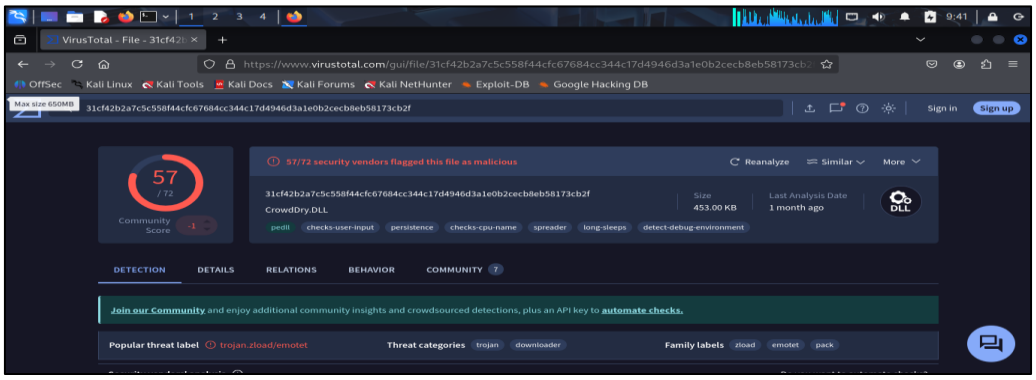

Figura 1. *Resultado de analizar el archivo 'invest_20.dll' en la página web 'VirusTotal'.*

De los 72 vendors con los que VirusTotal analiza los archivos 57 de estos, aproximadamente un 80%, clasifican este archivo como malicioso, siendo las clasificaciones más comunes las de 'troyano' y 'downloader'. Esto implica que la naturaleza de este ejecutable consiste en infectar sigilosamente equipos en los que a su vez introduce nuevos programas maliciosos y de no haber sido detectado a tiempo podría haber causado daños considerables en los equipos infectados.