Maestría en Ciberseguridad

Trabajo previo a la obtención de título de

Magister de Ciberseguridad

AUTOR/ES:

Diana Gabriela Lata Aguirre

Milton Javier Martínez Avilés

Christian Andrés Quiranza Estrella

Jonnathan Iván Torres Cruz

TUTOR:

Alejandro Cortés López

Análisis y Desarrollo de Técnicas para el Desbloqueo de Contenido en Euro Truck Simulator 2: Un Enfoque desde la Ciberseguridad

Quito – Ecuador

REINVENTEMOS EL FUTURO

Análisis y Desarrollo de Técnicas para el Desbloqueo de Contenido en Euro Truck Simulator 2: Un Enfoque desde la Ciberseguridad

Resumen

Este trabajo ha consistido en un análisis del videojuego Euro Truck Simulator2, combinando ingeniería inversa dinámica y estática. Con el objetivo de desarrollar técnicas para el desbloqueo de contenido. Inicialmente comenzamos justificando la elección del juego basándonos en su popularidad, presencia de comunidades activas, existencia de DLCs locales, destacando la vulnerabilidad del juego al permitir la edición de sus archivos guardados (como game.sii). Posteriormente, investigando la organización del contenido en archivos .scs dentro del directorio del juego y analizaremos la red con wireshark para conocer su comunicación del juego con el steam y su sincronización con la nube.. Luego utilizamos herramientas de ingeniería inversa para analizar steamapii.dll e identificamos la función steamapi_init() como punto de inicio de la conexión del juego con la API de steam, rastreamos eurotrucks2.exe como invoca esta función, revelando la presencia de “cheks vX”. Este proceso nos ha permitido identificar la vulnerabilidad principal en la manipulación de datos, también puntos en el código binario (exe o dll) donde aplicamos un parcheo permanente con el uso de Ghidra. Finalmente, modificando los valores con el depurador cheat engine para el desbloqueo de contenido.

Abstract

This work consisted of an analysis of Euro Truck Simulator 2, combining dynamic and static reverse engineering. The goal was to develop techniques for unlocking content. Initially, we started by justifying the choice of the game based on its popularity, presence of active communities, and existence of local DLCs. We highlighted the game's vulnerability in allowing editing of its save files (such as game.sii). Subsequently, we investigated the organization of content in .scs files within the game directory and analyzed the network with Wireshark to