Departamento de Ciencias de la Computación
Universidad de las Fuerzas Armadas - ESPE

Ensayo Colaborativo de Mapas Mundiales de Ciberataques en Tiempo Real

Parcial No. 1

Nombres:
Yeshua Amador Chiliquinga Amaya
Cesar Ignacio Loor Mercado

Carrera / Asignatura: Ingeniería de Software / Ingeniería de Seguridad de Software
NRC: 2540
Nombre del profesor: Walter Fuertes, PhD

Fecha de presentación: 26 de mayo del 2025

Mapas Mundiales de Ciberataques en Tiempo Real: Funcionamiento y Registro de Información

27 de mayo de 2025

En la era digital, la seguridad cibernética se ha convertido en una preocupación primordial para gobiernos, empresas y usuarios individuales. Los ciberataques son cada vez más frecuentes y sofisticados, lo que ha llevado al desarrollo de herramientas avanzadas para su detección y análisis. Entre estas herramientas se encuentran los mapas mundiales de ciberataques en tiempo real, que ofrecen una representación visual de las amenazas cibernéticas a medida que ocurren en diferentes partes del mundo.

Estos mapas recopilan datos de diversas fuentes, como sensores de red, sistemas de detección de intrusos y honeypots (sistemas diseñados para atraer ataques y analizarlos). Empresas como Kaspersky, Norse y Radware han desarrollado plataformas que visualizan estos datos en tiempo real, mostrando la ubicación geográfica de los ataques, su origen, destino y tipo.

Por ejemplo, el mapa de Kaspersky utiliza datos de su red global de usuarios para mostrar infecciones de malware, campañas de spam y otras amenazas cibernéticas. Los datos se actualizan constantemente, permitiendo a los usuarios observar patrones y tendencias en la actividad cibernética global.

Detrás de estos mapas se encuentran tecnologías avanzadas de recopilación y análisis de datos. Los sistemas de Gestión de Información y Eventos de Seguridad (SIEM, por sus siglas en inglés) juegan un papel crucial al consolidar y analizar grandes volúmenes de datos de seguridad en tiempo real. Estos sistemas permiten correlacionar eventos, generar alertas y proporcionar una visión integral de la postura de seguridad de una organización.

Además, se utilizan técnicas de visualización de datos para representar la información de manera comprensible y atractiva. Esto facilita la identificación rápida de patrones anómalos y la toma de decisiones informadas en materia de seguridad.

La información recopilada por estos sistemas se almacena en bases de datos especializadas que permiten su análisis posterior. Se registran detalles como la dirección IP del atacante, la hora del ataque, el tipo de amenaza y las acciones tomadas en respuesta. Este registro es esencial para realizar análisis forenses, mejorar las defensas cibernéticas y cumplir con requisitos regulatorios.

Es importante destacar que, para proteger la privacidad de los usuarios, muchas plataformas anonimizan los datos recopilados, eliminando información que pueda identificar

a individuos o entidades específicas.

Los mapas mundiales de ciberataques en tiempo real son herramientas valiosas para monitorear y comprender la dinámica de las amenazas cibernéticas. Aunque presentan ciertas limitaciones, su capacidad para visualizar y analizar ataques en tiempo real los convierte en recursos esenciales en la lucha contra el cibercrimen. Es fundamental complementar su uso con otras estrategias y tecnologías de seguridad para lograr una protección integral en el entorno digital.