



GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

BOARDROOM EXECUTIVE REPORT

ORGANO JUDICIAL

December 18, 2023



Organo Judicial 12/18/2023

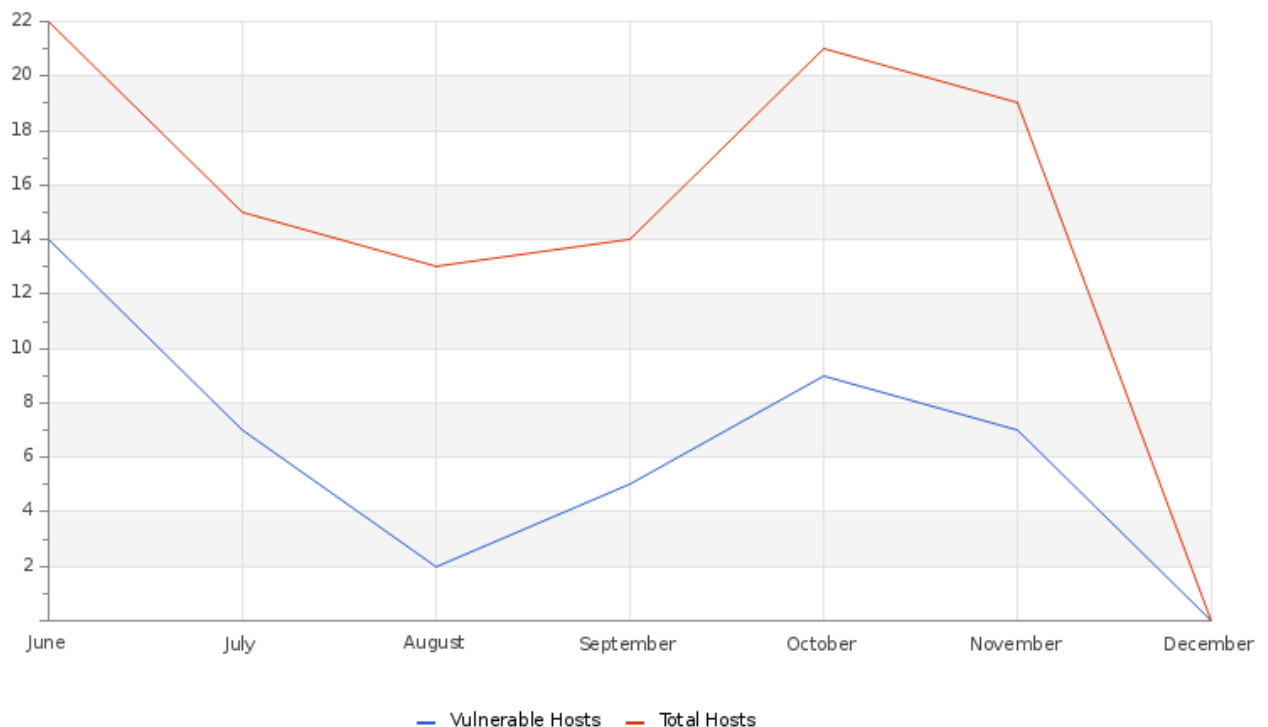
TLP AMBER BOARDROOM EXECUTIVE REPORT

Este informe corresponde a "Noviembre" y está dirigido al director o vicepresidente de TI, Ciberseguridad, Cumplimiento de Ciberseguridad o equivalente. La información está distribuida siguiendo el Modelo de seguridad cibernética de siete elementos de GLESEC (7eCSMTM), estos elementos son: Riesgo, Vulnerabilidades, Amenazas, Activos, Cumplimiento, Validación de Ciberseguridad y Acceso.

ABOUT THIS REPORT

El propósito de este documento es informar sobre el estado de seguridad para su organización. Debe ser notado que GLESEC basa su información en el análisis de los servicios bajo contrato. La información generada por estos servicios es entonces agregados, correlacionados y analizados.

Hosts & Vulnerable Hosts In Last 6 Months



El gráfico muestra una ligera disminución del número de hosts descubiertos, así como de las vulnerabilidades presentes en ellos. Entre las vulnerabilidades descubiertas se encuentran el uso de cifrados débiles y protocolos obsoletos como TLS 1.0. Recomendamos realizar los cambios pertinentes para mejorar la seguridad de la empresa u organización.

Organo Judicial 12/18/2023

Total Attacks Successfully Blocked

314876

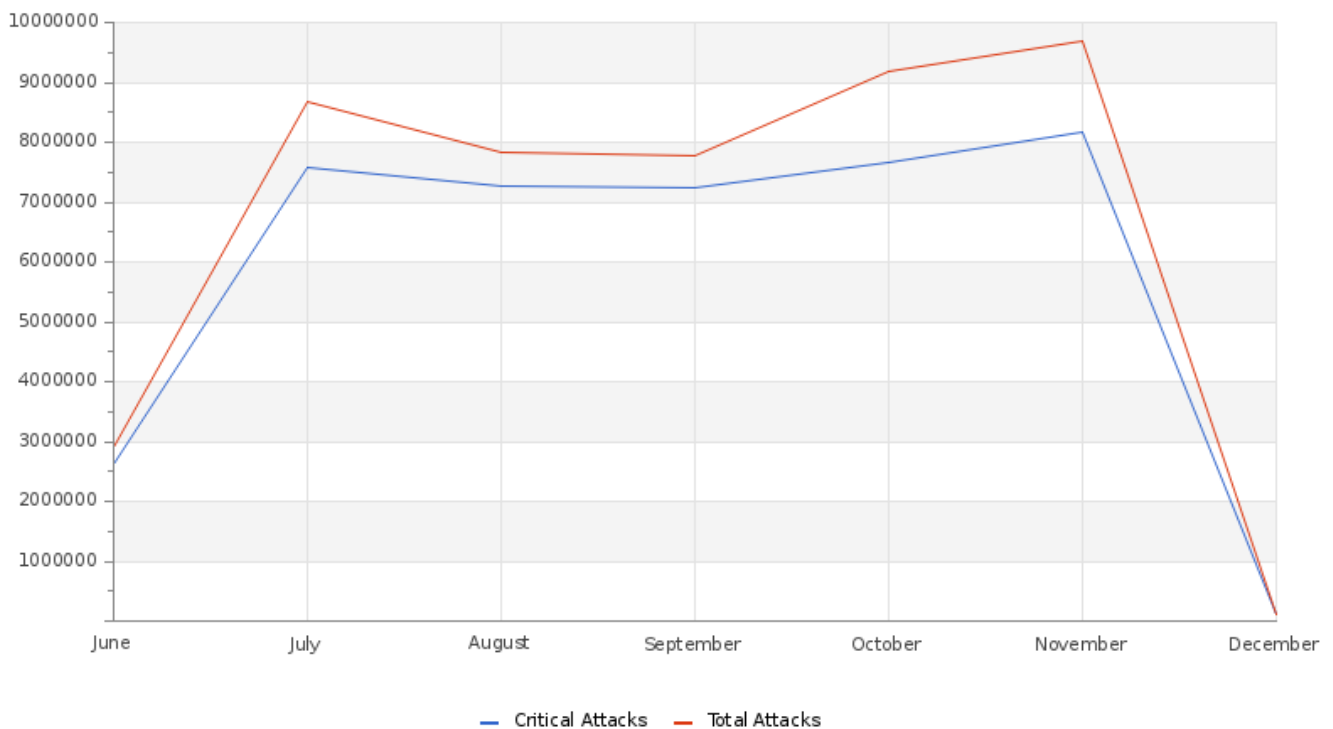
Durante el mes un total de 314,876 ataques fueron bloqueados de manera exitosa. A raíz de estos ataques se generaron casos de ataques persistentes, los cuales fueron documentados con las direcciones IP que realizaron múltiples ataques contra sus sistemas. Cabe destacar que la mayor parte de estos ataques proviene de direcciones IP maliciosas y Botnets.

Critical Attacks Successfully Blocked

301045

Un total de 301,045 ataques críticos fueron bloqueados de manera exitosa a lo largo del mes. La mayor parte de estos ataques han sido clasificados como ErtFeed y GeoFeed. Estas son configuraciones que se realizan en los equipos con el fin de robustecer la seguridad.

Attacks Successfully Blocked



En el transcurso del mes se registraron un total de 9,697,603 ataques. A través de un constante monitoreo se han identificado ataques de persistencia. Estos ataques provienen de IP's maliciosas y Botnets.

Organo Judicial 12/18/2023

Vulnerability Metric**2**

Se han identificado vulnerabilidades a nivel externo y hemos documentados casos para cada una de estas con sus respectivas recomendaciones para su mitigación. De un total de 19 host examinados, 7 presentaron vulnerabilidades. Según su severidad estas fueron clasificadas en 2 críticas, 2 altas, 13 medias y 1 baja. Para acceder a la documentación diríjase al apartado de casos en la sección de C&RU en SKYWATCH.

TLP:AMBER = Limited disclosure, restricted to participants' organizations. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**





GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

BOARDROOM EXECUTIVE REPORT

HOW CAN WE HELP?

Contact us today for more information on
our services and security solutions.

