TLP:AMBER

BOARDROOM EXECUTIVE REPORT

ORGANO JUDICIAL

March 07, 2024

Organo Judicial 03/07/2024

TLP AMBER BOARDROOM

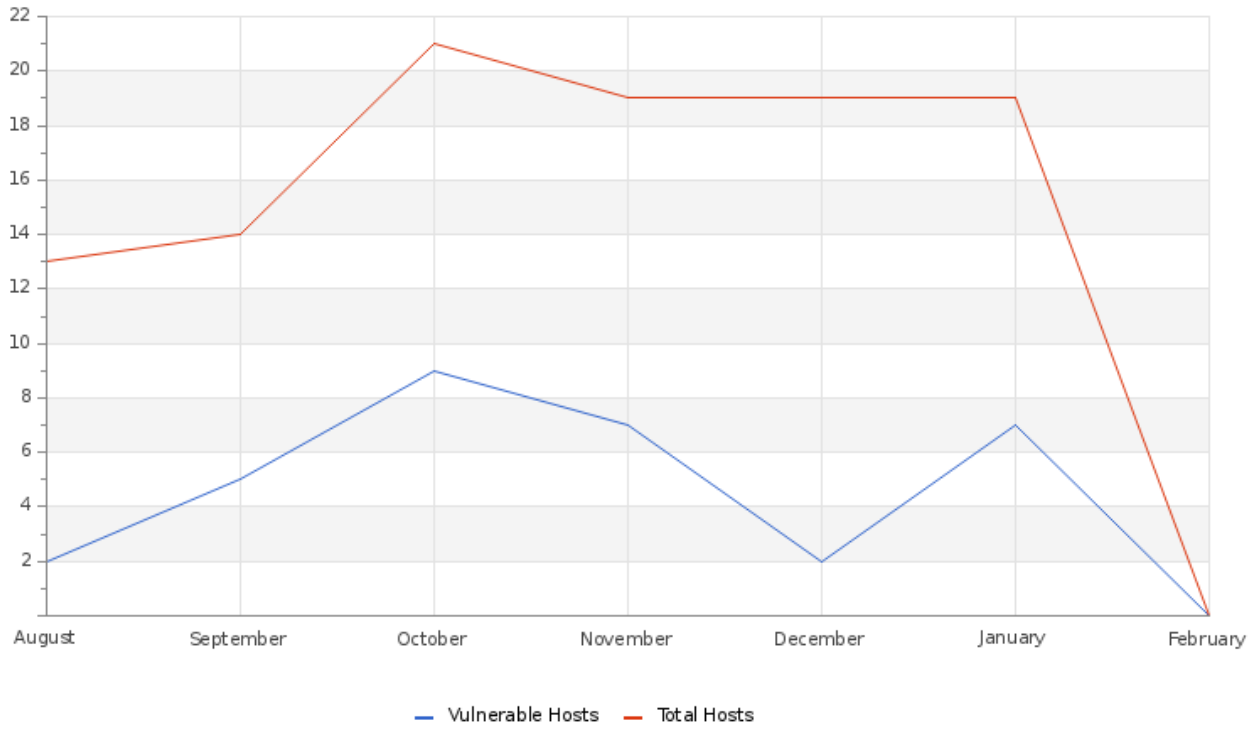
EXECUTIVE REPORT

Este informe corresponde a "Enero" 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 agregada, correlacionada y analizada.

Hosts & Vulnerable Hosts In Last 6 Months



El grafico muestra un ligero aumento en la cantidad de host que presentan vulnerabilidades, sin embargo para este mes la cantidad de host no varia. Las vulnerabilidades presentes se deben al uso de protocolos en desuso como lo es TLS 1.0 y el uso de sistemas operativos que ya no cuentan con soporte. Recomendamos realizar los cambios pertinentes para mejorar la seguridad de su organización.

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

Organo Judicial 03/07/2024

Total Attacks Successfully Blocked

176327

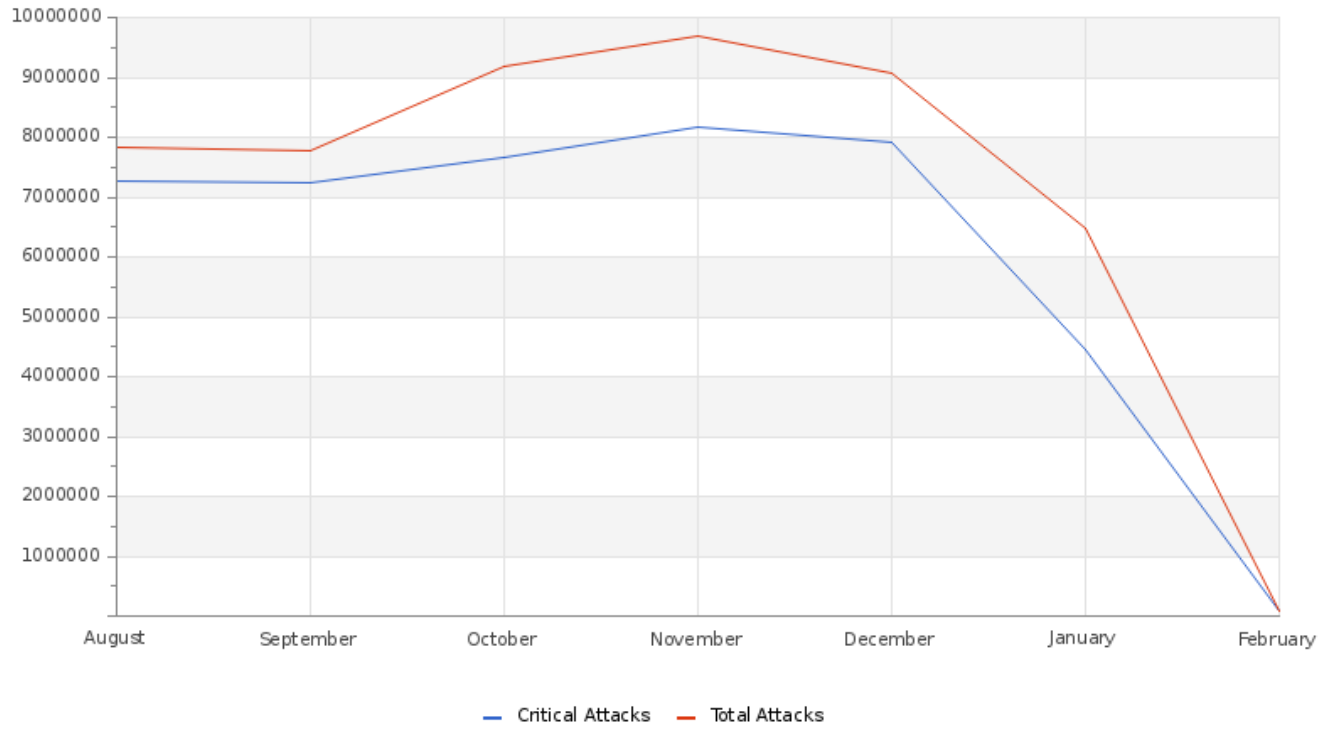
Durante el mes un total de 176,327 ataques fueron bloqueados de manera exitosa. Debido a la gran cantidad de ataques realizados contra sus sistemas, se generaron casos de ataques persistente, estos casos fueron documentados y se proporcionaron las direcciones IP desde las cuales se realizaron estos ataques. Cabe destacar que la mayor parte de estos ataques proviene de direcciones IP maliciosas y Botnets.

Critical Attacks Successfully Blocked

127420

A lo largo del mes un total de 127,420 ataques críticos fueron bloqueados de manera exitosa. 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 registro un total de 6,461,542 ataques de los cuales 4,461,515 fueron clasificados como críticos. A través de un constante monitoreo se pudieron identificar ataques de persistencia, los cuales suelen provenir de IP maliciosas que acumulan múltiples reportes y botnets.

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

Organo Judicial 03/07/2024

Vulnerability Metric

3

Se ha realizado actualizaciones para aquellas vulnerabilidades que persisten en sus sistemas. De un total de 19 host examinados, 7 presentaron vulnerabilidades. Según su severidad estas fueron clasificadas en 2 criticas, 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.**

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

TLP:AMBER

BOARDROOM EXECUTIVE REPORT

HOW CAN WE HELP?

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

LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500