TLP:AMBER

BOARDROOM EXECUTIVE REPORT

ORGANO JUDICIAL

March 09, 2024

Organo Judicial 03/09/2024

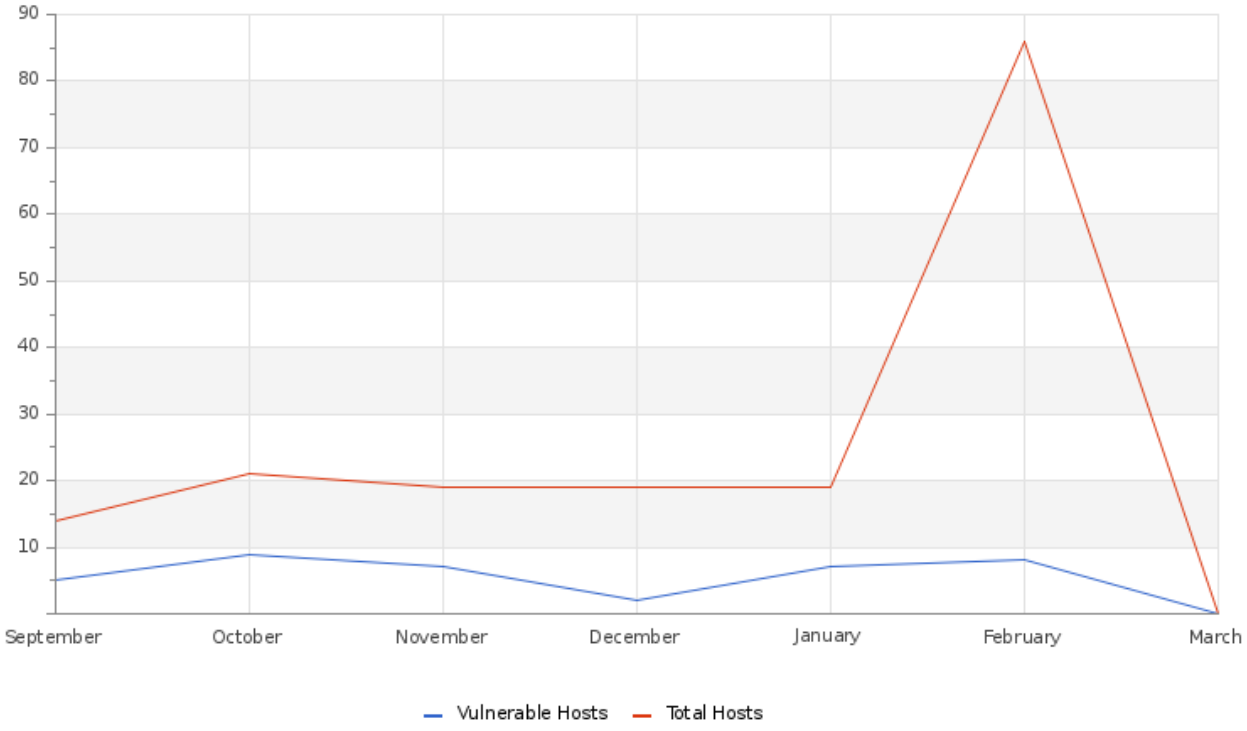
TLP AMBER BOARDROOM
EXECUTIVE REPORT

Este informe corresponde a "Febrero" 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



Se puede observar un aumento significativo en el total de host descubiertos durante el mes, mientras la cantidad de hosts con vulnerabilidades se mantiene. Las vulnerabilidades descubiertas durante el mes corresponden al uso de protocolos como TLS 1.0 y el uso de sistemas operativos que ya no cuentan con soporte.

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

Organo Judicial 03/09/2024

Total Attacks Successfully Blocked

207992

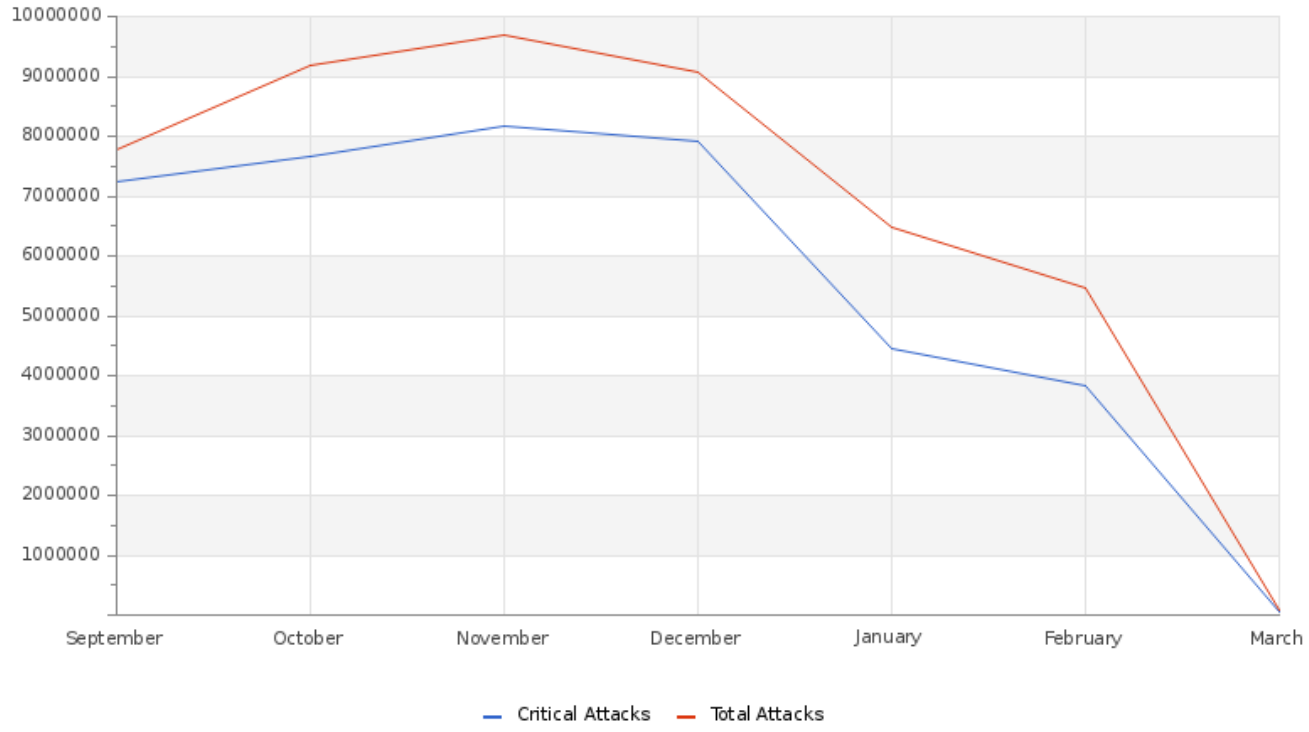
Durante el mes un total de 207,992 fueron bloqueados de manera exitosa, productos de estos ataques se generaron casos de persistencias, estos fueron documentados y se proporcionaron las direcciones IPs las cuales contaban con múltiples reportes de actividad maliciosa.

Critical Attacks Successfully Blocked

158524

Para los ataques clasificados como críticos, un total de 158,524 fueron bloqueados satisfactoriamente. La mayor parte de estos ataques han sido clasificados como ErtFeed y GeoFeed. Estas son configuraciones adicionales que se realizan en los equipos con el fin de robustecer la seguridad.

Attacks Successfully Blocked



A lo largo del mes como lo muestra la grafica se registraron un total del 5,460,275 ataques de los cuales 3,835,804 fueron clasificados como críticos. Producto de un constante monitoreo se pudieron identificar ataques de persistencias provenientes de IPs maliciosas que acumulan múltiples reportes y botnets.

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

Organo Judicial 03/09/2024

Vulnerability Metric

0

Se realizaron verificaciones de la vulnerabilidades que persisten en sus sistemas. De un total de 87 host examinados, 8 presentaron vulnerabilidades. Según su severidad estas fueron clasificadas en 6 criticas, 8 altas, 20 medias y 2 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