TLP:AMBER

BOARDROOM EXECUTIVE REPORT

ORGANO JUDICIAL

April 05, 2024

Organo Judicial 04/05/2024

TLP AMBER BOARDROOM

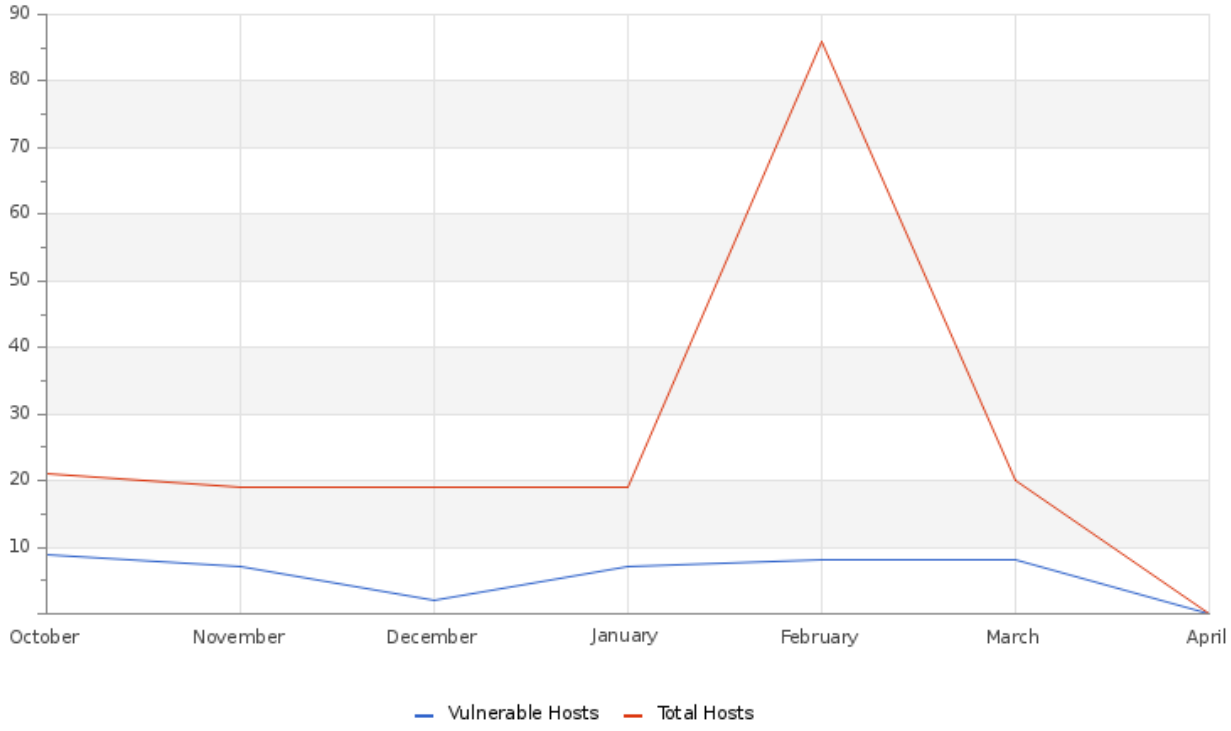
EXECUTIVE REPORT

Este informe corresponde a Marzo 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



La grafica muestra una disminución significativa en la cantidad de hosts descubiertos durante el mes, sin embargo la cantidad de hosts vulnerables se mantienen. Las vulnerabilidades descubiertas durante el mes corresponden a servidores con software sin soporte y el uso de protocolos en desuso.

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

Organo Judicial 04/05/2024

Total Attacks Successfully Blocked

181857

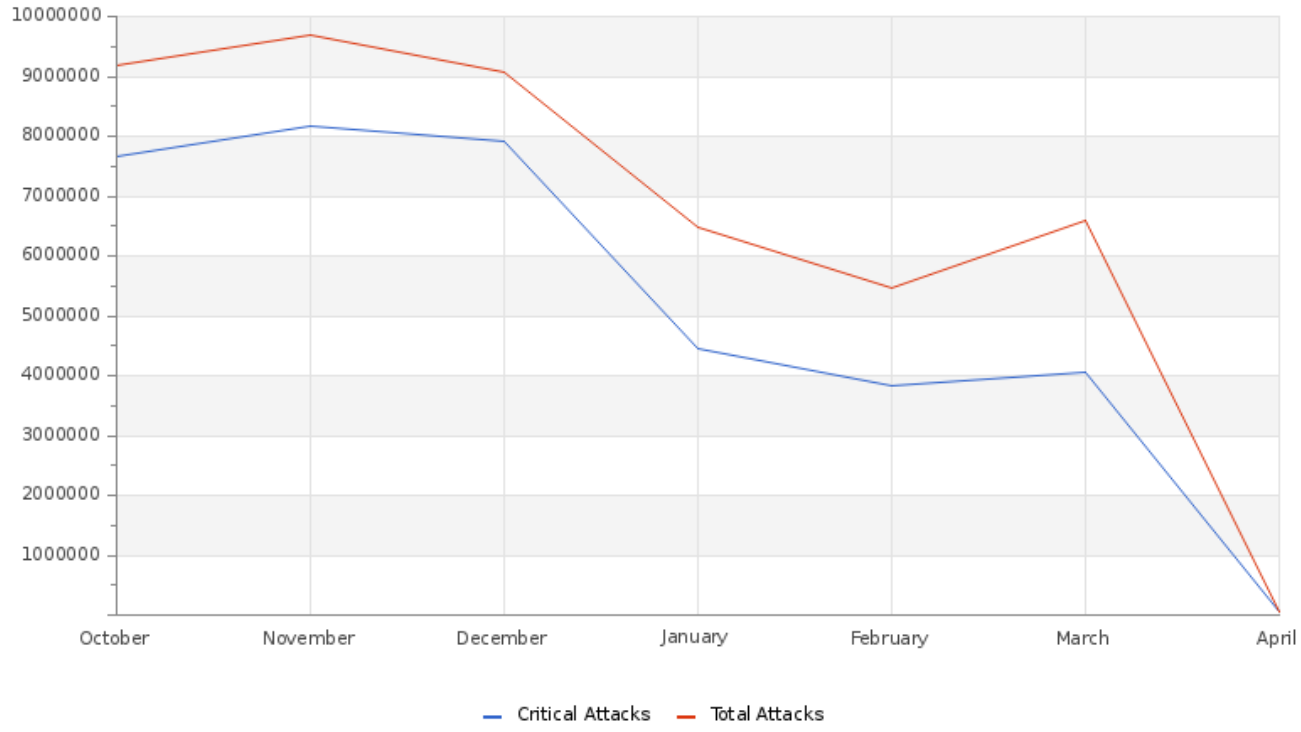
Durante el mes un total de 181,857 fueron bloqueados de manera exitosa, productos de estos ataques se generaron casos de persistencia. Se documentaron casos en donde se incluyen las direcciones IP desde donde se realizaban estos ataques. Hemos verificado estas direcciones y presentan múltiples reportes por actividad maliciosa.

Critical Attacks Successfully Blocked

140024

Para los ataques clasificados como críticos, un total de 140,024 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 DefensePro con el fin de robustecer la seguridad.

Attacks Successfully Blocked



Durante el mes se registraron un total de 6,574,325 ataques, de los cuales 4,060,949 fueron catalogados como críticos. Producto de un constante monitoreo se identificaron ataques de persistencia provenientes de IP que acumulan múltiples reportes por actividad maliciosa.

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

Organo Judicial 04/05/2024

Vulnerability Metric

3

Se verificaron las vulnerabilidades que persisten en sus sistemas. De un total de 20 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