TLP:AMBER

BOARDROOM EXECUTIVE REPORT

ORGANO JUDICIAL

October 18, 2023

Organo Judicial 10/18/2023

TLP AMBER BOARDROOM

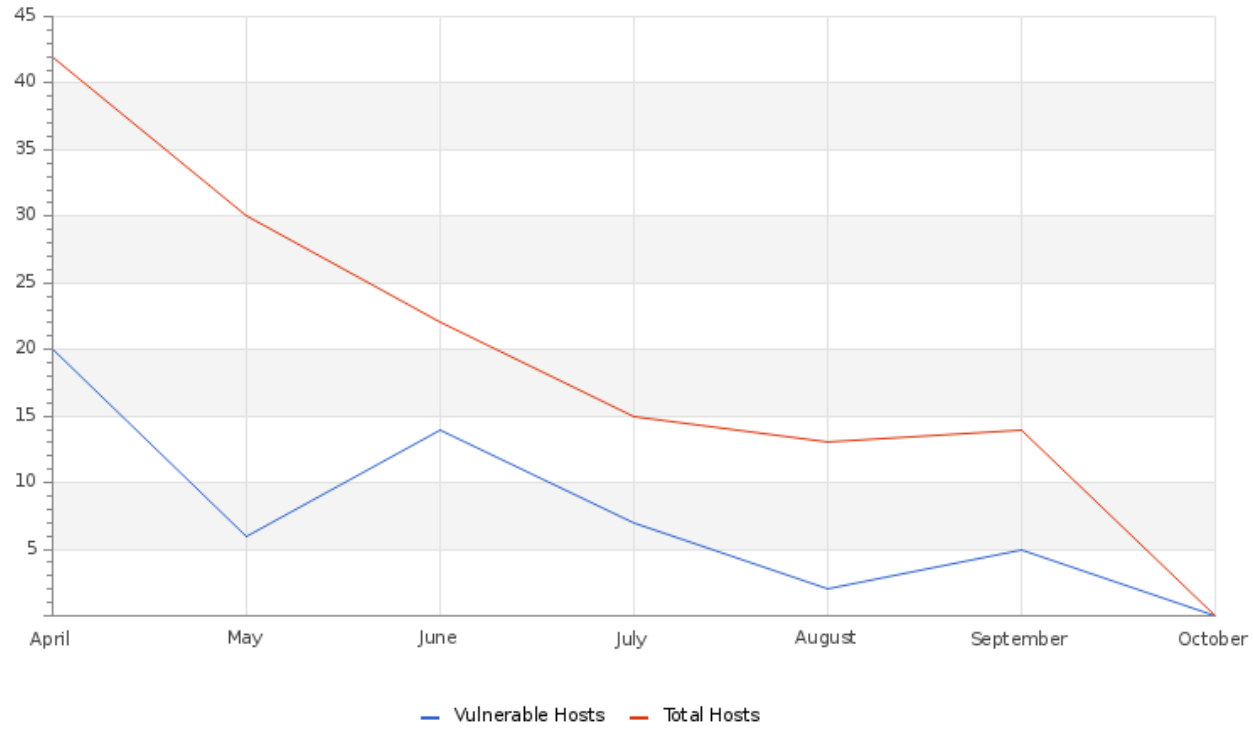
EXECUTIVE REPORT

Este informe corresponde "Septiembre" 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



En la grafica se puede observar un leve aumento en los hosts descubiertos durante el mes y los hosts que presentan vulnerabilidades. Entre las vulnerabilidades descubiertas se encuentra el uso de protocolos en desuso en algunos sistemas y componentes de sistemas operativos desactualizados. Recomendamos hacer uso de versiones recientes de estos protocolos y realizar las actualizaciones pertinentes para mejorar de la seguridad de su empresa u organización.

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

Organo Judicial 10/18/2023

Total Attacks Successfully Blocked

199700

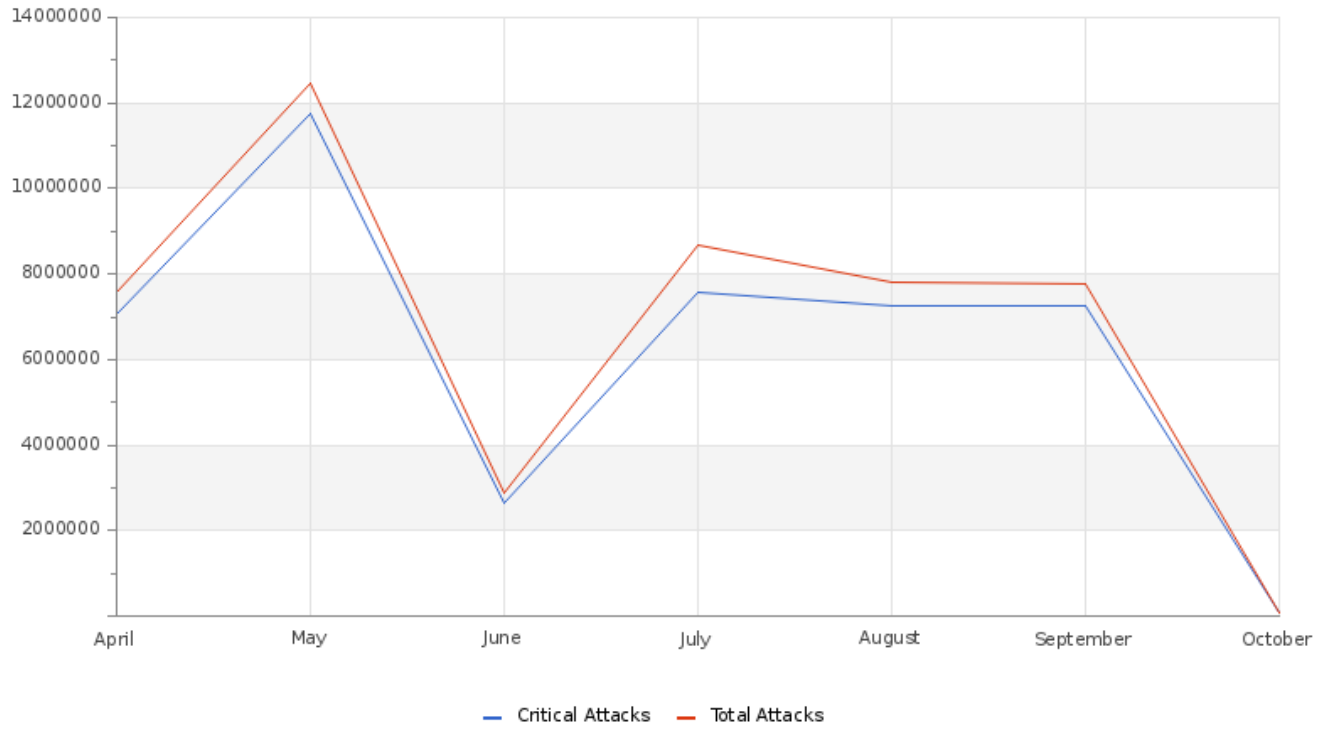
Durante el mes un total de 199,700 fueron detectados y bloqueados de manera exitosas, estos ataques se dirigieron a múltiples sistemas de su organización. Producto del monitoreo constante y una respuesta inmediata fueron generados casos de ataques persistentes durante el mes. Cabe destacar que la mayor parte de estos ataques proviene de direcciones IP maliciosas y Botnets.

Critical Attacks Successfully Blocked

187631

Un total de 187,631 ataques críticos se registraron durante el mes, estos ataques fueron bloqueados de manera efectiva. La mayor parte de estos ataques son clasificados como ErtFeed y GeoFeed. Ambas son configuraciones adicionales que tiene como objetivo robustecer la seguridad.

Attacks Successfully Blocked



A lo largo del mes se registraron en total 7,766,228 ataques. Hemos estado monitoreando estas actividades de manera constante con el fin de identificar ataques de persistencia. La mayor parte de los ataques provienen de IP's maliciosas y Botnets.

LATAM HQ
+507 836-5355

US HQ
+1 (321) 430-0500

Organo Judicial 10/18/2023

Vulnerability Metric

3

Hemos identificado vulnerabilidades a nivel externo y proporcionado recomendaciones para su mitigación. De un total de 14 direcciones que se examinaron, 5 presentaban vulnerabilidades. Según el grado de severidad estas fueron clasificadas en 2 criticas, 2 altas, 9 medias y 1 baja. Estas vulnerabilidades han sido documentadas y se encuentran disponibles en la sección C&RU de 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