

TLP:AMBER

BOARDROOM EXECUTIVE REPORT

TROPIGAS

November 11, 2026



©2023. GLESEC. All Rights Reserved.

TROPIGAS 11/11/2026

TLP AMBER BOARDROOM

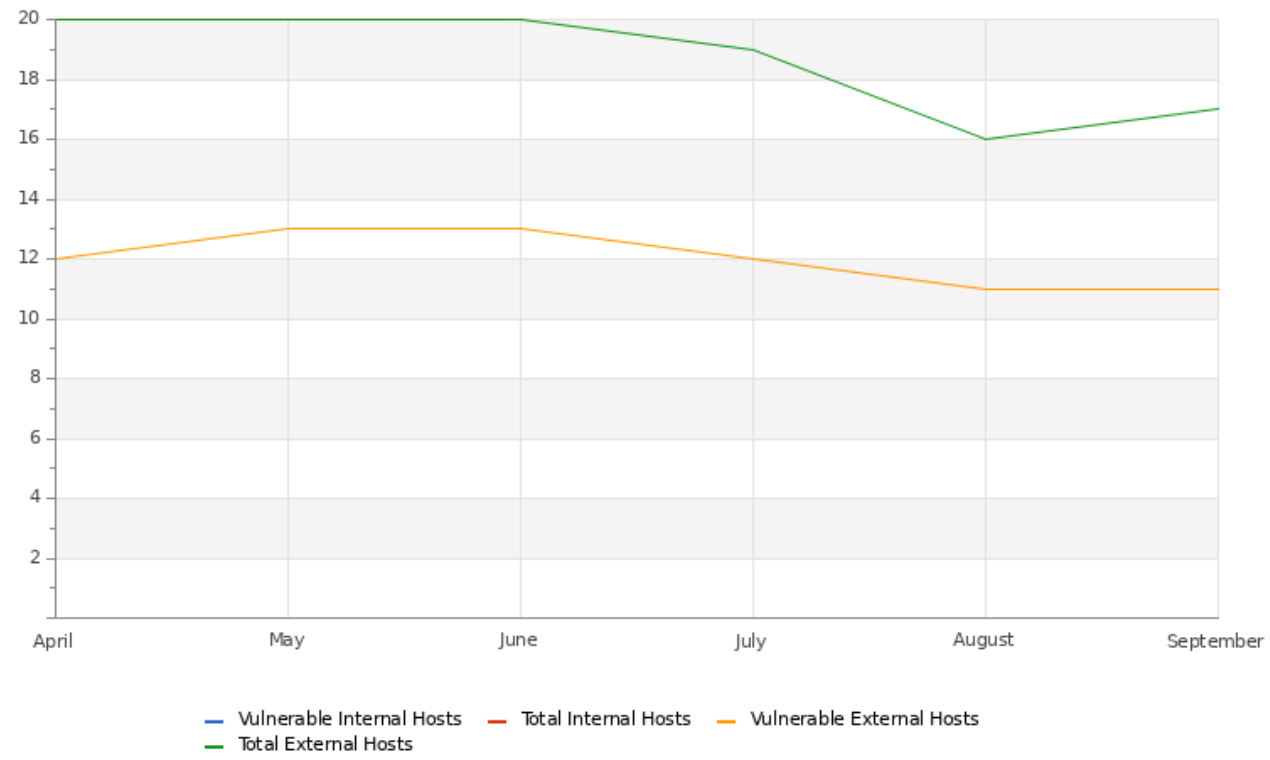
EXECUTIVE REPORT

Este informe corresponde "AGOSTO 2026" 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.

SOBRE ESTE INFORME

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



Durante los últimos seis meses se observa una reducción reciente tanto en la cantidad de sistemas descubiertos como en los hosts con vulnerabilidades. Para agosto, se identificaron 16 sistemas expuestos a Internet, de los cuales 11 presentan vulnerabilidades activas. Asimismo, la tendencia de vulnerabilidades muestra un total de 25, distribuidas en 17 de severidad media y 8 de severidad baja, sin identificarse vulnerabilidades de severidad alta o crítica. Esta evolución refleja una disminución de las vulnerabilidades externas identificadas; sin embargo, la permanencia de vulnerabilidades medias y bajas en los activos identificados requiere mantener las acciones de remediación y seguimiento para continuar disminuyendo la superficie de ataque.

©2023. GLESEC. All Rights Reserved.

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

TROPIGAS 11/11/2026

Total Attacks Successfully Blocked

50497816

Durante el mes de agosto se registraron 545,594 eventos de seguridad, frente a los 6,028,677 registrados en julio, lo que representa una reducción aproximada del 90.95 %. Este comportamiento refleja una disminución considerable en el volumen de eventos recibidos. A pesar de las validaciones internas realizadas por GLESEC sobre la ingesta y el procesamiento de la información para descartar posibles inconvenientes de nuestro lado, se identificaron cambios importantes tanto en el volumen como en el tipo de eventos registrados entre ambos períodos. Es importante señalar que el valor de 50,497,816 eventos corresponde al acumulado de los últimos 90 días, por lo que no representa exclusivamente la actividad registrada durante agosto. Asimismo, GLESEC no administra directamente la consola de Radware y su visibilidad se basa en la información recibida a través de la API. Por este motivo, se recomienda realizar una revisión conjunta con el cliente desde la consola de Radware, con el objetivo de contrastar la información de origen con los eventos recibidos por GLESEC y determinar con mayor precisión la causa de esta reducción.

Critical Attacks Successfully Blocked

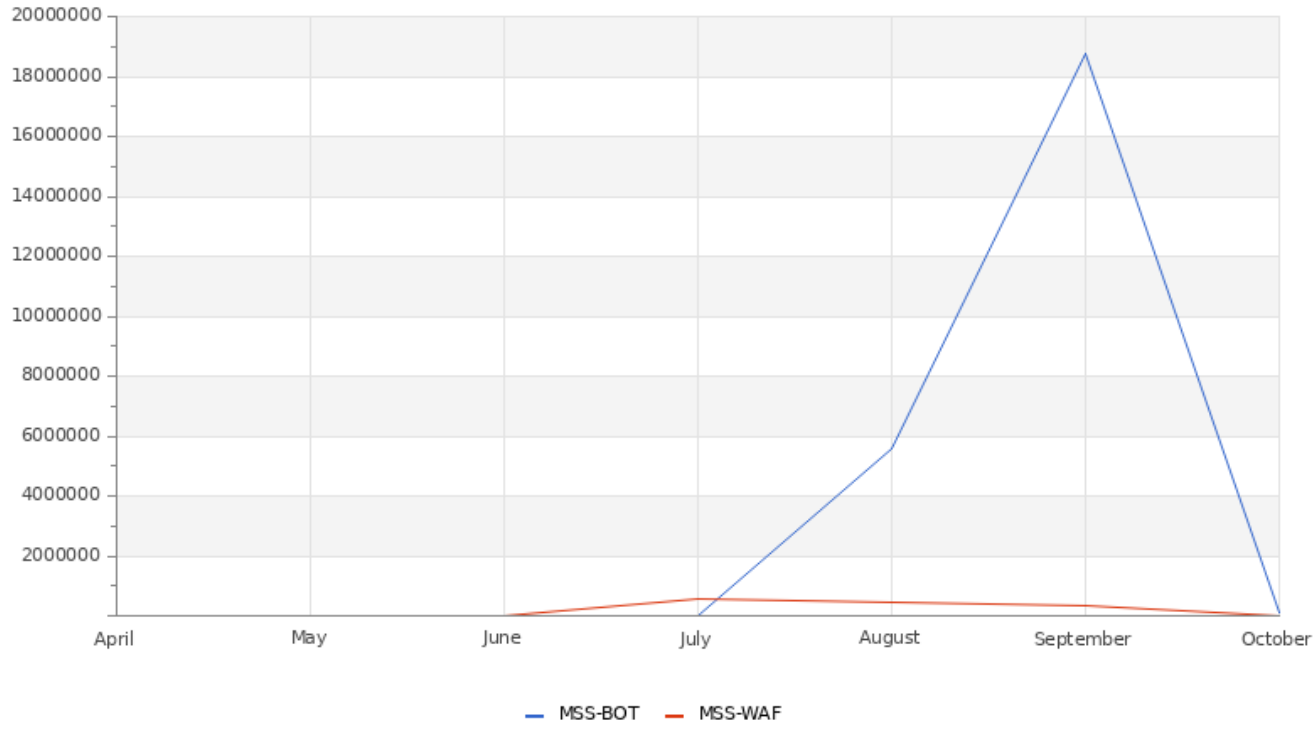
1394475

Durante el mes de agosto se registraron 545,594 eventos de seguridad, frente a 591,415 registrados en julio, representando una reducción aproximada del 7.75 %. Esta variación evidencia una disminución en el volumen de actividad registrada durante el período evaluado. Los controles de seguridad lograron gestionar los eventos identificados, contribuyendo a la protección de los activos y servicios protegidos. De igual forma, el valor de 1,394,475 eventos corresponde al acumulado de más de 30 días, por lo que no representa exclusivamente la actividad registrada durante agosto.

Attacks Successfully Blocked

©2023. GLESEC. All Rights Reserved.
PROPRIETARY & CONFIDENTIAL

TROPIGAS 11/11/2026



Durante el mes de agosto se registraron 545,594 eventos de seguridad WAF, frente a los 6,028,677 registrados en julio, lo que representa una reducción aproximada del 90.95 %. Por otro lado, los eventos correspondientes a BOT Protection, analizados de manera independiente de los WAF Security Events, registraron un total de 16,422,735 durante agosto, evidenciando un incremento respecto al mes anterior. Este comportamiento refleja una evolución diferenciada entre ambas categorías: mientras los eventos WAF presentaron una disminución considerable, la actividad BOT registró un incremento durante el mismo período. Esta variación evidencia cambios en el volumen de actividad registrada; sin embargo, los mecanismos de seguridad permitieron gestionar los eventos identificados.

Vulnerability Metric

8

El análisis de la superficie externa identificó 16 sistemas expuestos a Internet, de los cuales 11 presentan vulnerabilidades activas, con un total de 25 vulnerabilidades externas: 17 de severidad media y 8 de severidad baja, sin hallazgos críticos ni altos. Las principales debilidades están relacionadas con configuraciones de servicios web, protocolos criptográficos obsoletos, certificados digitales y exposición de información. Entre los hallazgos identificados, la vulnerabilidad ICMP Timestamp Request Remote Date Disclosure presentó la mayor recurrencia, siendo detectada en cinco activos. Aunque estos hallazgos no presentan una criticidad elevada de manera individual, su presencia puede ampliar la superficie de ataque y proporcionar información útil para actividades de reconocimiento, por lo que se recomienda fortalecer las configuraciones de seguridad de los servicios web, actualizar los protocolos criptográficos, mantener los certificados digitales vigentes y restringir la exposición innecesaria de información.

TLP:AMBER

©2023. GLESEC. All Rights Reserved.
PROPRIETARY & CONFIDENTIAL

TROPIGAS 11/11/2026

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.**

©2023. GLESEC. All Rights Reserved.

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.

©2023. GLESEC. All Rights Reserved.

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