TLP:AMBER

BOARDROOM EXECUTIVE REPORT

TROPIGAS

August 19, 2026

©2023. GLESEC. All Rights Reserved.

TROPIGAS 08/19/2026

TLP AMBER BOARDROOM

EXECUTIVE REPORT

Este informe corresponde "JULIO 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

Total Attacks Successfully Blocked

13567718

Durante el período evaluado, los mecanismos de seguridad bloquearon exitosamente un total de 13,567,718 intentos de ataque, evidenciando un volumen elevado de actividad dirigida contra los activos y servicios expuestos de la organización.

Los eventos identificados pueden estar asociados con diferentes tipos de actividad, incluyendo tráfico automatizado, intentos de reconocimiento, exploración de recursos, validación de servicios expuestos y posibles intentos de explotación. El volumen registrado refleja una actividad constante sobre la superficie de ataque monitoreada, lo que resalta la importancia de mantener controles preventivos y capacidades de detección activas.

A pesar de la cantidad de eventos registrados, los mecanismos de seguridad lograron detectar y bloquear exitosamente la actividad identificada, reduciendo el riesgo de accesos no autorizados, explotación de vulnerabilidades o afectaciones sobre los servicios protegidos.

©2023. GLESEC. All Rights Reserved.
PROPRIETARY & CONFIDENTIAL
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TROPIGAS 08/19/2026

Critical Attacks Successfully Blocked

664779

Durante el período evaluado se registraron 664,779 ataques clasificados como críticos, los cuales fueron bloqueados exitosamente por los controles de seguridad implementados. Estos eventos representan aproximadamente el 4.90 % del total de ataques bloqueados, evidenciando una presencia significativa de actividad con mayor nivel de riesgo.

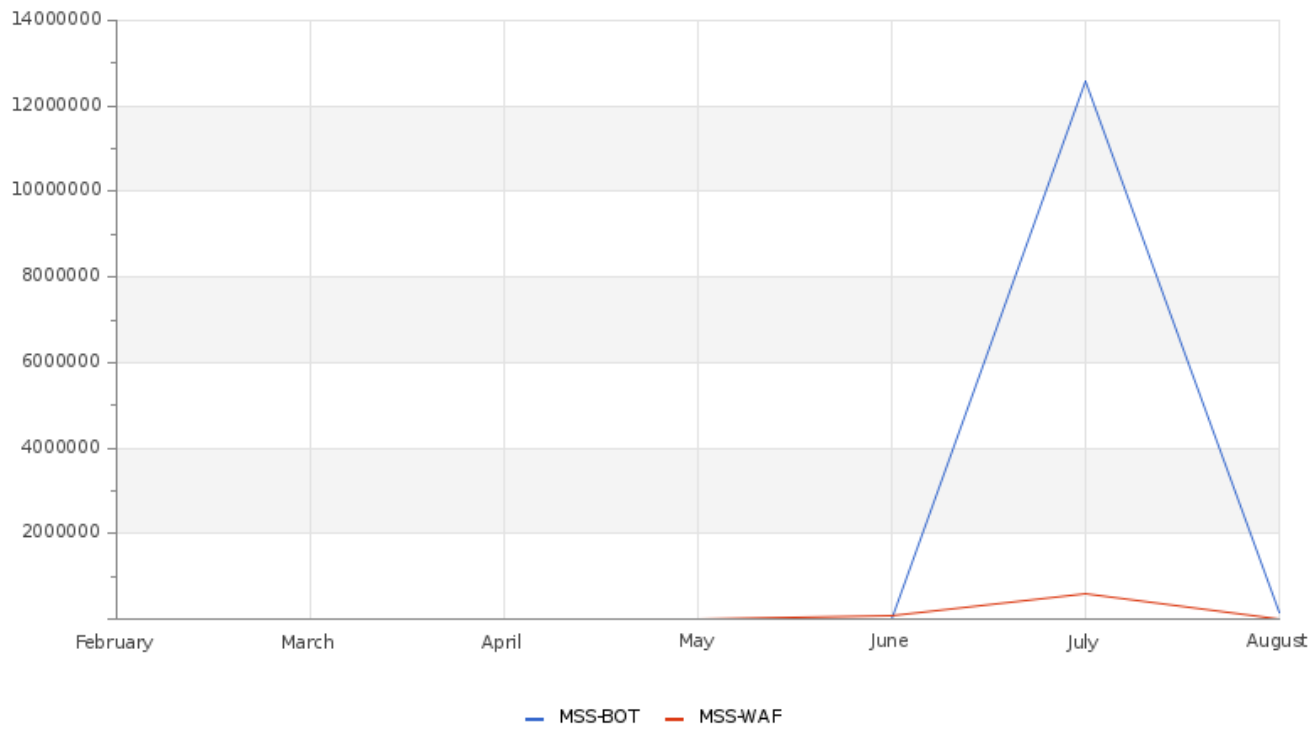
Entre las categorías con mayor incidencia se identificaron Attackers Feed, Endpoint Reconnaissance, Geo-Blocking, Server Information Leakage, Rate Limiting y URL Access Violation. Estas detecciones se encuentran principalmente relacionadas con actividades de reconocimiento, identificación de servicios expuestos, recopilación de información, accesos desde ubicaciones restringidas y generación automatizada de solicitudes contra los recursos publicados.

Este tipo de comportamiento puede formar parte de etapas iniciales de reconocimiento y búsqueda de posibles vectores de ataque. Sin embargo, los mecanismos de protección permitieron identificar y bloquear oportunamente estas actividades, disminuyendo la posibilidad de que evolucionaran hacia intentos de explotación, acceso no autorizado o compromiso de los activos monitoreados.

©2023. GLESEC. All Rights Reserved.
PROPRIETARY & CONFIDENTIAL
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TROPIGAS 08/19/2026

Attacks Successfully Blocked



Durante el período evaluado se registró un incremento significativo en la actividad de ataques bloqueados, destacando el servicio MSS-BOT con aproximadamente 12.6 millones de eventos mitigados, mientras que MSS-WAF bloqueó alrededor de 664 mil intentos de ataque. Este comportamiento evidencia una elevada presencia de tráfico automatizado, actividades de reconocimiento y solicitudes potencialmente maliciosas dirigidas contra aplicaciones y servicios expuestos a Internet. A pesar del volumen observado, los mecanismos de protección demostraron una respuesta efectiva, bloqueando oportunamente la actividad identificada y reduciendo el riesgo de afectación sobre la infraestructura monitoreada. En conjunto, los resultados reflejan la efectividad de los servicios MSS-BOT y MSS-WAF frente a amenazas automatizadas y ataques dirigidos a la capa de aplicación.

©2023. GLESEC. All Rights Reserved.
PROPRIETARY & CONFIDENTIAL
LATAM HQ
+507 836-5355
US HQ
+1 (321) 430-0500

TROPIGAS 08/19/2026

Vulnerability Metric

5

El análisis de los 19 activos evaluados durante el período evidencia que la cantidad de hosts con vulnerabilidades identificadas se mantuvo estable en 12, sin variaciones respecto al período anterior. En total, se identificaron 30 vulnerabilidades, de las cuales 22 corresponden a severidad media y 8 a severidad baja, manteniendo la métrica general de vulnerabilidades en un 5 %.

Aunque los resultados reflejan un nivel de exposición relativamente controlado y sin incremento en la cantidad de activos afectados, la permanencia de vulnerabilidades de severidad media indica que aún existen condiciones que podrían ser aprovechadas para ampliar la superficie de ataque o comprometer determinados servicios expuestos.

Por este motivo, se recomienda continuar fortaleciendo las actividades de gestión y remediación, priorizando aquellas vulnerabilidades con mayor impacto potencial sobre la infraestructura. Asimismo, resulta conveniente mantener evaluaciones periódicas de seguridad y un monitoreo continuo de los activos expuestos, con el objetivo de reducir progresivamente la exposición identificada y fortalecer la postura general de ciberseguridad de la organización.

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