TLP:AMBER

BOARDROOM EXECUTIVE REPORT

TROPIGAS

August 20, 2026

TROPIGAS 08/20/2026

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 mes de julio se registraron 6,028,677 ataques bloqueados, frente a 2,483,937 registrados en junio, lo que representa un incremento aproximado del 142.7 %. Este comportamiento refleja un aumento considerable en el volumen de actividad maliciosa dirigida contra los activos y servicios de la organización. A pesar del incremento observado, los controles de seguridad implementados lograron bloquear la actividad identificada, reduciendo la exposición de los recursos protegidos ante los diferentes vectores de ataque. Es importante señalar que el valor de 13,567,718 ataques bloqueados corresponde al acumulado de los últimos 90 días, por lo que no representa exclusivamente la actividad registrada durante julio.

Critical Attacks Successfully Blocked

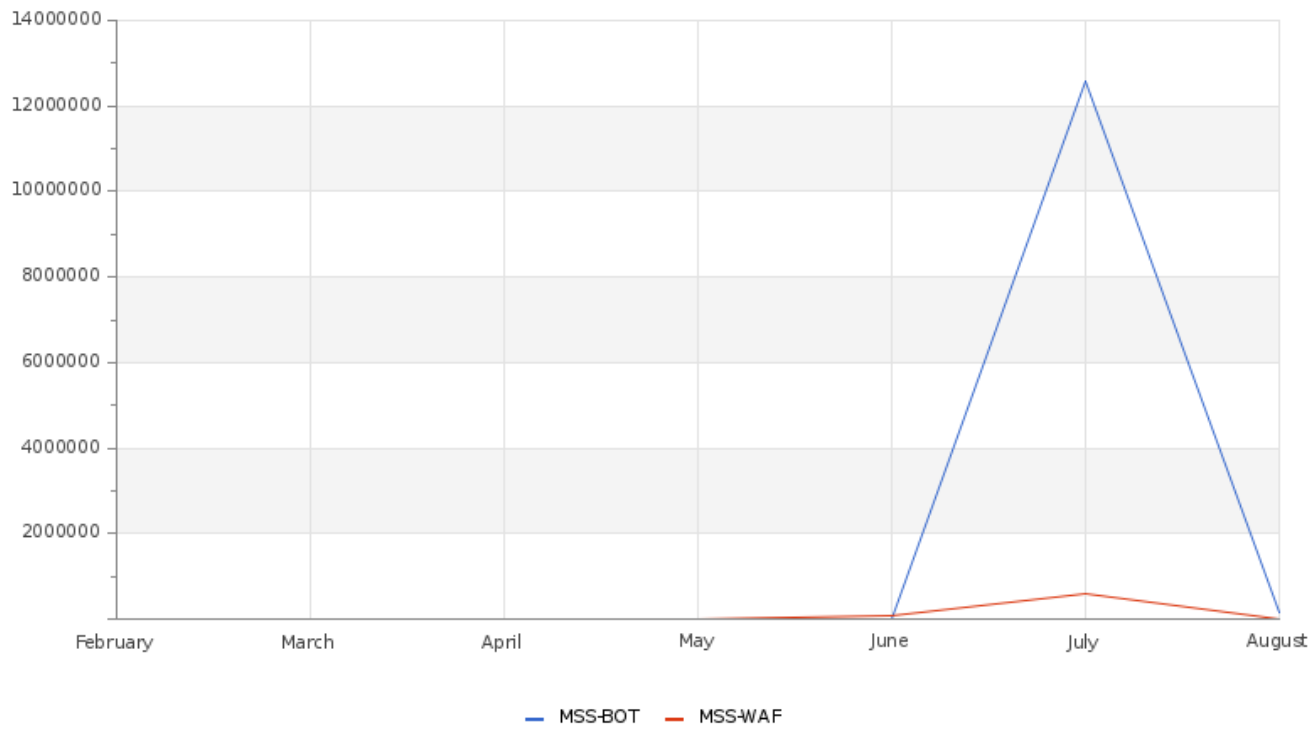
664779

Durante el mes de julio se registraron 591,415 ataques críticos bloqueados, frente a 66,936 registrados en junio, representando un incremento aproximado del 783.5 %. Adicionalmente, los eventos críticos pasaron de representar aproximadamente el 2.69 % del total de ataques en junio al 9.81 % en julio, evidenciando no solo un incremento en el volumen de actividad, sino también una mayor concentración de ataques clasificados con nivel de riesgo crítico. Los controles de seguridad lograron bloquear estos eventos, evitando que la actividad identificada alcanzara los activos y servicios protegidos. De igual forma, el valor de 664,779 ataques críticos bloqueados corresponde al acumulados de mas de 30 dias.

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

TROPIGAS 08/20/2026

Attacks Successfully Blocked



Durante el mes de julio se registraron 6,028,677 ataques bloqueados, frente a 2,483,937 registrados en junio, lo que representa un incremento aproximado del 142.7 %. La actividad observada estuvo asociada a los controles de MSS-BOT y MSS-WAF, que permitieron identificar y bloquear solicitudes maliciosas y tráfico automatizado dirigido contra las aplicaciones y servicios protegidos. Este incremento evidencia una mayor actividad durante julio; sin embargo, los mecanismos de seguridad lograron contener los eventos identificados. Es importante señalar que los valores superiores mostrados en algunos indicadores corresponden a acumulados de períodos más amplios, por lo que el total utilizado para el análisis mensual de julio es de 6,028,677 ataques bloqueados.

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

TROPIGAS 08/20/2026

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.**

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