TLP:AMBER

BOARDROOM EXECUTIVE REPORT

TROPIGAS

July 30, 2026

TLP AMBER BOARDROOM

EXECUTIVE REPORT

Este informe corresponde "MAYO 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.

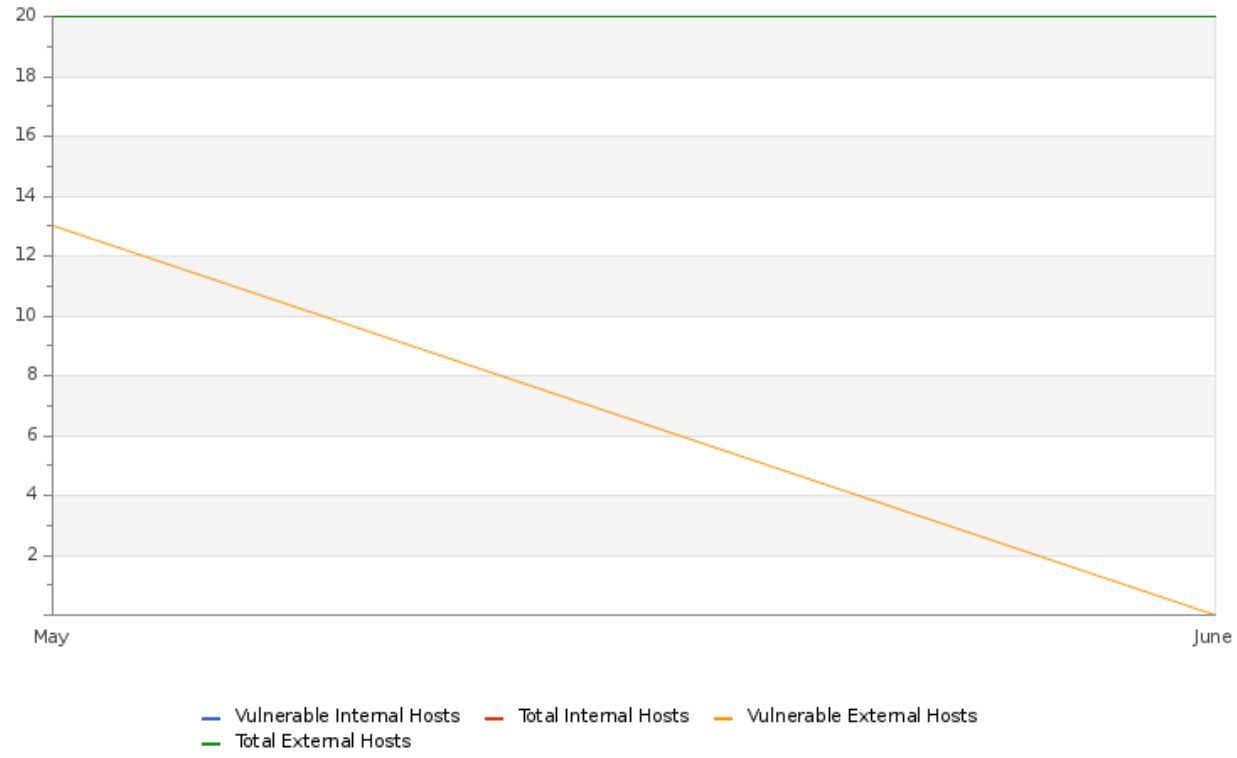
SOBRE ESTE INFORME

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.

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

TROPIGAS 07/30/2026

Hosts & Vulnerable Hosts In Last 6 Months



Durante el mes de mayo se evaluó un total de 20 hosts externos. En comparación con el período anterior, la cantidad de activos con vulnerabilidades identificadas se mantuvo estable en 12 hosts, lo que indica que la superficie de exposición de la organización no presentó variaciones significativas durante el período evaluado. No obstante, la identificación de vulnerabilidades en estos activos pone de manifiesto la necesidad de mantener un proceso continuo de gestión y remediación para reducir el riesgo asociado. La métrica general de vulnerabilidades se mantiene en un nivel controlado, lo que refleja la efectividad de las actividades de monitoreo y evaluación implementadas. Se recomienda continuar fortaleciendo el proceso de gestión de vulnerabilidades mediante evaluaciones periódicas, la remediación priorizada de los hallazgos de mayor criticidad y el monitoreo constante de los activos expuestos, con el objetivo de disminuir progresivamente la superficie de ataque y fortalecer la postura de seguridad de la organización.

Total Attacks Successfully Blocked

16189891

Durante el período evaluado, los mecanismos de seguridad bloquearon exitosamente un total de 16,189,891 intentos de ataque, lo que representa un incremento significativo con respecto al mes anterior. Este comportamiento evidencia un aumento en la actividad maliciosa dirigida contra los activos expuestos de la organización, incluyendo intentos de reconocimiento, explotación de vulnerabilidades y tráfico automatizado. A pesar del mayor volumen de eventos, los controles de seguridad implementados mantuvieron un desempeño eficaz, detectando y mitigando oportunamente las amenazas identificadas, lo que permitió preservar la disponibilidad, integridad y seguridad de la infraestructura monitoreada.

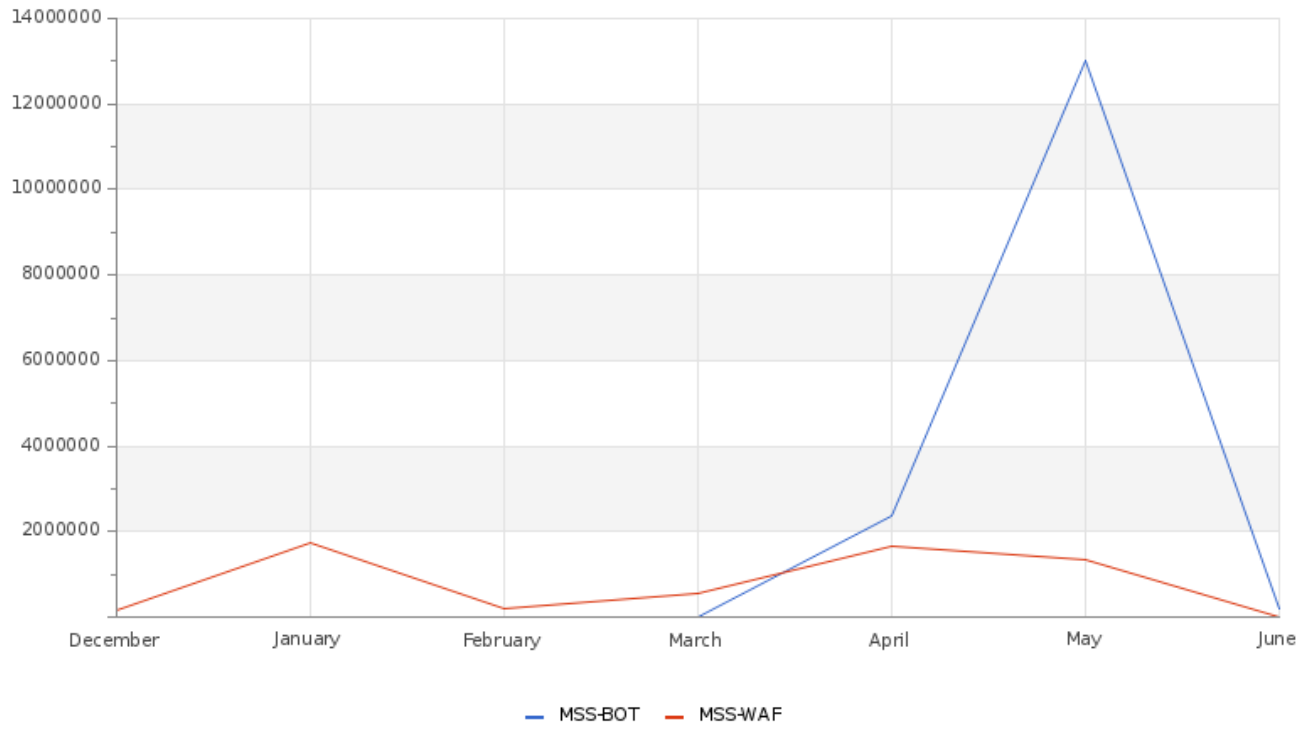
TROPIGAS 07/30/2026

Critical Attacks Successfully Blocked

3446827

A nivel de ataques críticos, durante el mes de abril se registró un total de 3,446,827 eventos bloqueados. La categoría con mayor incidencia fue Attackers Feed, seguida de Endpoint Reconnaissance, Geo-Blocking, Server Information Leakage, Rate Limiting y URL Access Violation. Este comportamiento refleja un incremento en las actividades de reconocimiento, escaneo automatizado y búsqueda de vectores de explotación dirigidos contra los servicios expuestos de la organización. No obstante, los mecanismos de protección implementados demostraron una alta capacidad de detección y respuesta, permitiendo identificar y bloquear oportunamente estas amenazas antes de que pudieran comprometer los activos monitoreados. En consecuencia, se mantuvo una postura de seguridad robusta, mitigando eficazmente el riesgo asociado a este incremento en la actividad maliciosa y fortaleciendo la protección de la infraestructura tecnológica.

Attacks Successfully Blocked



Durante el mes de mayo se registró un incremento significativo en la actividad de ataques bloqueados, destacando el servicio MSS-BOT con aproximadamente 15 millones de eventos mitigados, mientras que el servicio MSS-WAF bloqueó cerca de 1.5 millones de intentos de ataque. Este comportamiento evidencia un aumento considerable en la actividad automatizada generada por bots maliciosos, así como una mayor cantidad de intentos de explotación dirigidos contra aplicaciones y servicios expuestos a Internet. La elevada actividad observada refleja un panorama de amenazas más dinámico, caracterizado por campañas automatizadas de reconocimiento, escaneo y explotación. No obstante, los mecanismos de protección implementados demostraron una alta capacidad de detección y respuesta, permitiendo bloquear oportunamente el tráfico malicioso y minimizar el riesgo de compromiso de la infraestructura. En conjunto, los resultados confirman la efectividad de las soluciones MSS-BOT y MSS-WAF para mitigar tanto ataques automatizados como amenazas dirigidas a la capa de aplicación, contribuyendo a preservar la disponibilidad, integridad y seguridad de los servicios monitoreados.

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

Vulnerability Metric

9

El análisis de los 20 activos evaluados durante el mes evidencia que la cantidad de hosts con vulnerabilidades identificadas se mantuvo estable en 12, sin variaciones respecto al período anterior. En total, se detectaron 14 vulnerabilidades, de las cuales 11 corresponden a severidad media y 3 a severidad baja, situando la métrica general de vulnerabilidades en un 9%. Si bien este resultado refleja una postura de riesgo moderada y un nivel de exposición controlado, la persistencia de vulnerabilidades de severidad media evidencia la necesidad de fortalecer las actividades de gestión y remediación para reducir la superficie de ataque. En este contexto, se recomienda priorizar la corrección de las vulnerabilidades de mayor impacto, mantener evaluaciones periódicas de seguridad y reforzar el monitoreo continuo de los activos expuestos, con el objetivo de disminuir progresivamente el nivel de riesgo y fortalecer la postura 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