TLP:AMBER

BOARDROOM EXECUTIVE REPORT

TROPIGAS

July 30, 2026

TROPIGAS 07/30/2026

TLP AMBER BOARDROOM

EXECUTIVE REPORT

Este informe corresponde "MARZO 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 el mes de marzo, el número total de hosts externos se ha mantenido estable en 15 a lo largo de los últimos tres meses. En contraste, la cantidad de hosts con vulnerabilidades ha presentado un leve incremento, pasando de 8 a 9. Este comportamiento indica que, aunque la infraestructura se mantiene constante, existe una ligera variación en el nivel de exposición que debe ser atendida. Aun así, las medidas de seguridad implementadas continúan mostrando efectividad en la contención de riesgos. Se recomienda mantener un monitoreo continuo y reforzar las prácticas de gestión de vulnerabilidades, con el fin de identificar oportunamente posibles debilidades y reducir el impacto de riesgos potenciales en el entorno.

Total Attacks Successfully Blocked

870900

Durante el período evaluado, se bloquearon exitosamente 870,900 intentos de ataque, lo que representa un incremento significativo en comparación con el mes anterior. Este aumento refleja una mayor actividad maliciosa en el entorno durante el período analizado. No obstante, los controles de seguridad demostraron un desempeño sólido, manteniendo su eficacia de forma consistente y asegurando un nivel adecuado de protección frente a las amenazas identificadas.

Critical Attacks Successfully Blocked

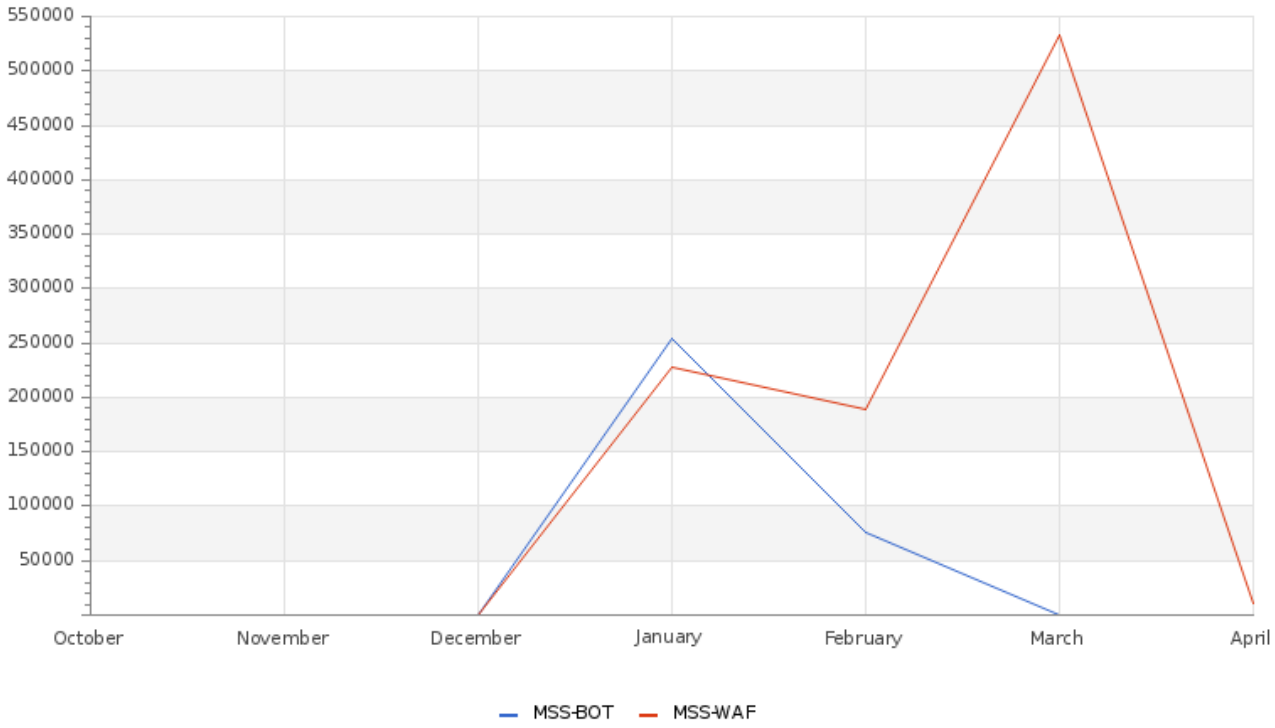
954727

A nivel de ataques críticos, durante el mes de marzo se registró un total de 954,727 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 evidencia una actividad constante de reconocimiento, escaneo automatizado e intentos de explotación dirigidos contra los servicios expuestos de la organización. No obstante, la activación y efectividad de los controles implementados por la plataforma de protección permitieron identificar y bloquear oportunamente estas amenazas, reduciendo el riesgo de compromiso de los activos monitoreados y fortaleciendo la postura de seguridad de la infraestructura.

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

TROPIGAS 07/30/2026

Attacks Successfully Blocked



Durante el mes de marzo se evidenció un incremento significativo en la actividad de ataques bloqueados por el servicio MSS-WAF, alcanzando el volumen más alto del período analizado, con más de 530 mil eventos mitigados. Este comportamiento refleja un aumento considerable en los intentos de explotación dirigidos contra aplicaciones web y servicios expuestos, lo que demuestra una mayor actividad de reconocimiento y escaneo automatizado por parte de actores maliciosos. En contraste, el servicio MSS-BOT no registró eventos relevantes durante el mes, lo que indica una disminución de la actividad asociada a bots automatizados. A pesar del incremento observado en los ataques orientados a aplicaciones web, los mecanismos de protección implementados lograron detectar y bloquear eficazmente las solicitudes maliciosas, contribuyendo a mantener la seguridad y disponibilidad de los servicios protegidos.

Vulnerability Metric

6

El análisis de los 15 activos evaluados durante el mes evidencia una variación mínima en la superficie de exposición, registrándose un incremento de 8 a 9 hosts con vulnerabilidades identificadas. En total, se detectaron 13 vulnerabilidades, de las cuales 10 corresponden a severidad media y 3 a severidad baja, manteniendo una métrica general de vulnerabilidades del 6%. Este resultado refleja una postura de riesgo controlada y un nivel de exposición reducido; sin embargo, pone de manifiesto la importancia de continuar con un proceso continuo de gestión de vulnerabilidades. Se recomienda priorizar la remediación de las vulnerabilidades de severidad media, fortalecer las actividades periódicas de evaluación y validación de seguridad, y mantener un monitoreo constante de los activos expuestos, con el fin de reducir progresivamente la superficie de ataque y preservar la integridad, disponibilidad y confidencialidad de la infraestructura tecnológica.

TROPIGAS 07/30/2026

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.**

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