TLP:AMBER

BOARDROOM EXECUTIVE REPORT

TROPIGAS

July 30, 2026

TROPIGAS 07/30/2026

TLP AMBER BOARDROOM

EXECUTIVE REPORT

Este informe corresponde "ABRIL 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 abril se evaluó un total de 20 hosts externos, evidenciándose un incremento en la cantidad de activos con vulnerabilidades identificadas, al pasar de 9 a 12 hosts respecto al mes anterior. Este comportamiento refleja un ligero aumento en la superficie de exposición de la organización, asociado a la identificación de nuevos hallazgos de seguridad durante el período. No obstante, la métrica general de vulnerabilidades se mantiene en un nivel controlado, lo que evidencia la efectividad de las actividades de monitoreo y gestión 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 continuo de los activos expuestos, con el objetivo de reducir progresivamente la superficie de ataque y mejorar la postura de seguridad de la organización.

Total Attacks Successfully Blocked

2593124

Durante el período evaluado, se bloquearon exitosamente 2,593,124 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

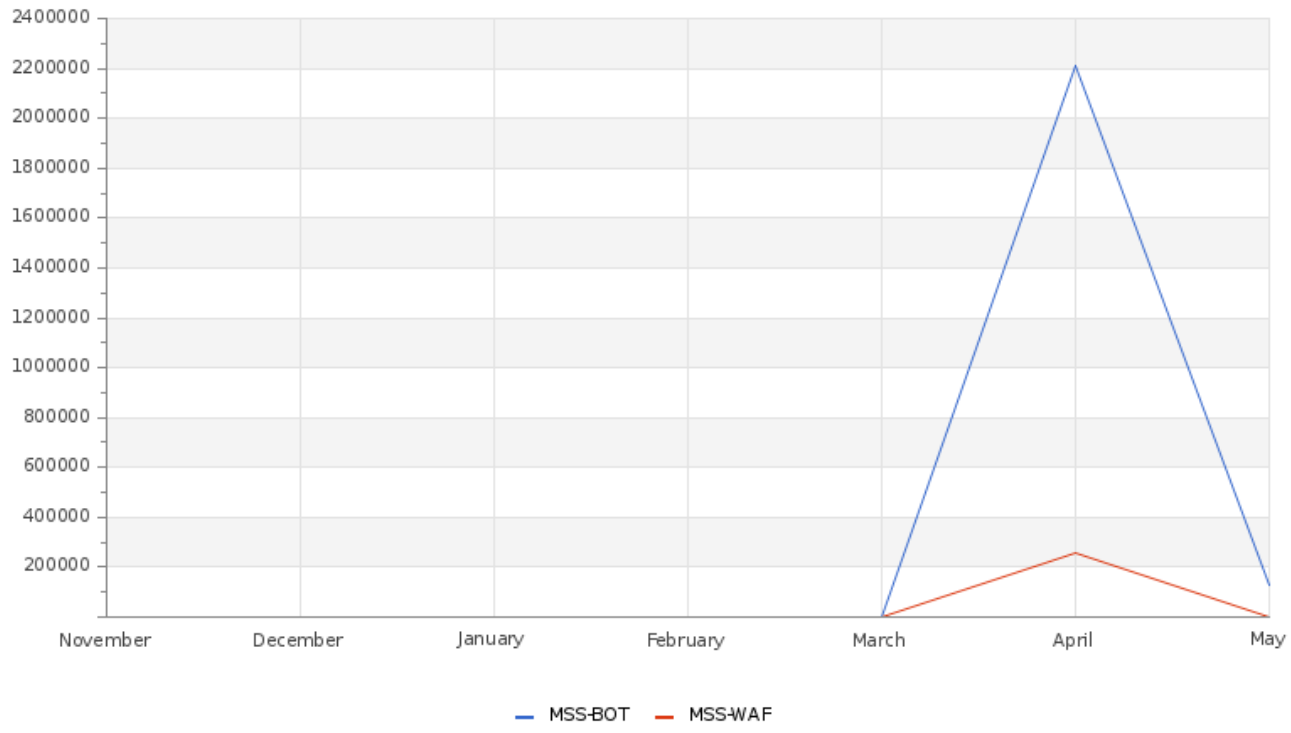
257751

A nivel de ataques críticos, durante el mes de marzo se registró un total de 257,751 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 abril se registró un incremento significativo en la actividad de ataques bloqueados, destacando el servicio MSS-BOT con aproximadamente 2.2 millones de eventos mitigados, mientras que el servicio MSS-WAF bloqueó alrededor de 250 mil ataques. Este comportamiento evidencia un aumento considerable en la actividad automatizada generada por bots maliciosos, la cual representa uno de los principales vectores de amenaza para los servicios expuestos a Internet. Asimismo, el volumen de eventos procesados por MSS-WAF refleja la persistencia de intentos de explotación dirigidos contra aplicaciones web, los cuales fueron detectados y bloqueados de manera oportuna por los controles de seguridad implementados. En conjunto, los resultados demuestran la efectividad de las soluciones de protección para mitigar tanto campañas automatizadas como ataques orientados a la capa de aplicación, contribuyendo a mantener la disponibilidad, integridad y seguridad de la infraestructura monitoreada.

Vulnerability Metric

7

El análisis de los 20 activos evaluados durante el mes evidencia un ligero incremento en la superficie de exposición, registrándose un aumento de 9 a 12 hosts con vulnerabilidades identificadas. En total, se detectaron 16 vulnerabilidades, distribuidas en 1 de severidad alta, 12 de severidad media y 3 de severidad baja, lo que sitúa la métrica general de vulnerabilidades en un 7%. Si bien este porcentaje refleja una postura de riesgo moderada y una exposición aún controlada, la incorporación de una vulnerabilidad de severidad alta incrementa el nivel de riesgo asociado a la infraestructura evaluada y requiere atención prioritaria. En este contexto, se recomienda implementar acciones de remediación enfocadas inicialmente en las vulnerabilidades de mayor criticidad, complementándolas con un proceso continuo de gestión de vulnerabilidades, evaluaciones periódicas de seguridad y monitoreo constante de los activos expuestos. Estas medidas contribuirán a reducir la superficie de ataque, fortalecer la postura de ciberseguridad de la organización y minimizar la probabilidad de explotación de vulnerabilidades por parte de actores maliciosos.

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