TLP:AMBER

BOARDROOM EXECUTIVE REPORT

TROPIGAS

July 30, 2026

TLP AMBER BOARDROOM

EXECUTIVE REPORT

Este informe corresponde "JUNIO 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 junio se evaluó un total de 19 hosts externos, observándose un ligero incremento en la cantidad de activos con vulnerabilidades identificadas, al pasar de 12 a 13 hosts respecto al período anterior. Este comportamiento refleja una variación moderada en la superficie de exposición de la organización, derivada de la identificación de nuevos hallazgos de seguridad durante las evaluaciones realizadas. Aunque el aumento es limitado, pone de manifiesto la necesidad de mantener un proceso continuo de gestión de vulnerabilidades para evitar un incremento progresivo del riesgo. En este contexto, se recomienda priorizar la remediación de las vulnerabilidades detectadas según su nivel de criticidad, realizar evaluaciones periódicas de seguridad y mantener un monitoreo constante de los activos expuestos. Estas acciones 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.

Total Attacks Successfully Blocked

13569994

Durante el período evaluado, los mecanismos de seguridad bloquearon exitosamente un total de 13,569,994 intentos de ataque, evidenciando un incremento en la actividad maliciosa respecto al mes anterior. Este comportamiento refleja una mayor intensidad en las campañas de reconocimiento, escaneo automatizado y ataques dirigidos contra los servicios expuestos de la organización. A pesar del aumento en el volumen de eventos, los controles de seguridad implementados mantuvieron un desempeño eficaz, permitiendo detectar y mitigar oportunamente las amenazas identificadas. Como resultado, se preservó la disponibilidad, integridad y seguridad de la infraestructura monitoreada, demostrando la efectividad de las capacidades de prevención y respuesta frente al incremento de la actividad maliciosa.

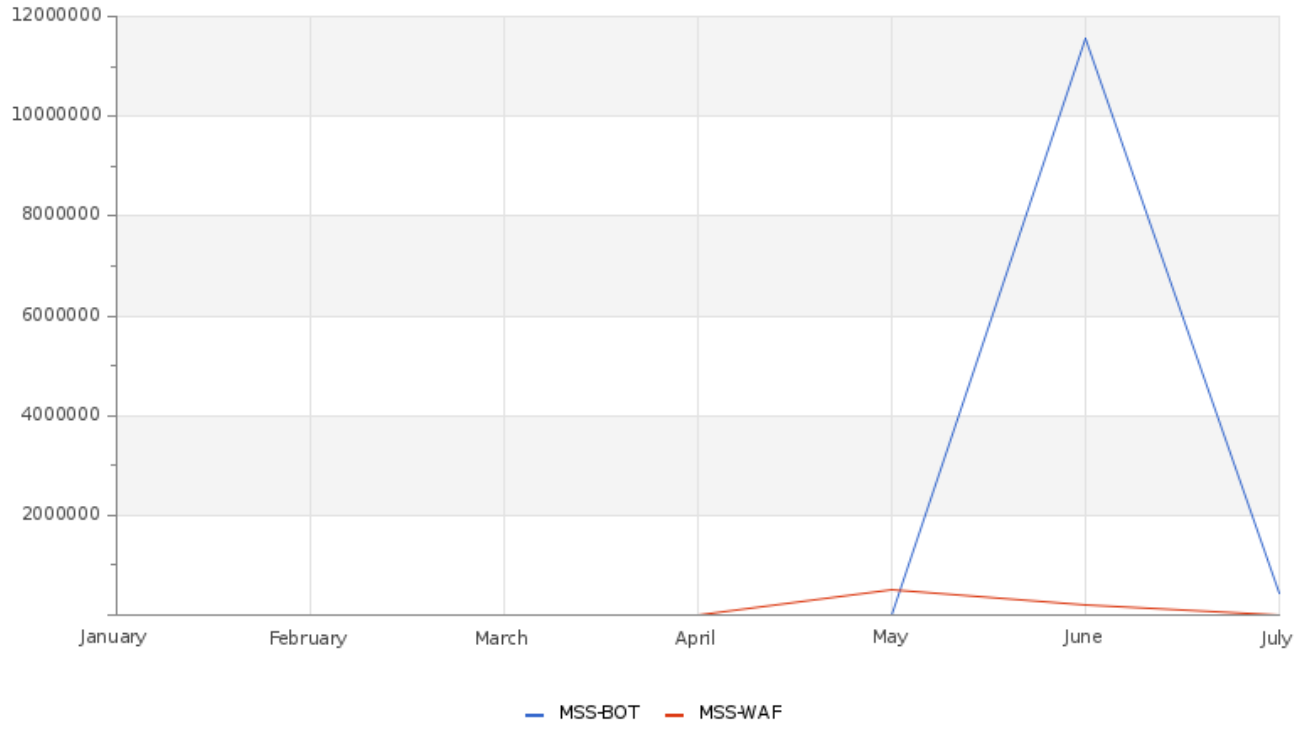
TROPIGAS 07/30/2026

Critical Attacks Successfully Blocked

717718

A nivel de ataques críticos, durante el período evaluado se registró un total de 717,718 eventos bloqueados. La categoría con mayor incidencia fue Attackers Feed, seguida por Geo-Blocking, Server Information Leakage, y URL Access Violation. Este comportamiento refleja una actividad sostenida de reconocimiento, escaneo automatizado e intentos de explotación dirigidos contra los servicios y aplicaciones expuestos a Internet, así como tráfico originado desde fuentes previamente asociadas con actividades maliciosas. No obstante, las capacidades de detección y protección implementadas permitieron identificar y bloquear oportunamente estas amenazas, mitigando el riesgo de compromiso de los activos monitoreados y contribuyendo a fortalecer la postura de ciberseguridad de la organización.

Attacks Successfully Blocked



Durante el mes de junio se registró un incremento extraordinario en la actividad de ataques bloqueados, destacando el servicio MSS-BOT con aproximadamente 11.5 millones de eventos mitigados, mientras que el servicio MSS-WAF bloqueó alrededor de 200 mil intentos de ataque. Este comportamiento evidencia un aumento considerable en la actividad automatizada generada por bots maliciosos, caracterizada por campañas masivas de reconocimiento, escaneo e intentos de explotación dirigidos contra los servicios expuestos a Internet. Aunque el volumen de eventos asociados a MSS-WAF fue significativamente menor, continuó detectando y bloqueando de forma efectiva intentos de ataque orientados a la capa de aplicación. En conjunto, los resultados demuestran la capacidad de las soluciones MSS-BOT y MSS-WAF para responder eficazmente ante un escenario de alta actividad maliciosa, mitigando el tráfico no autorizado y contribuyendo a preservar la disponibilidad, integridad y seguridad de la infraestructura monitoreada.

TROPIGAS 07/30/2026

Vulnerability Metric

7

El análisis de los 19 activos evaluados durante el mes evidencia un ligero incremento en la superficie de exposición, al registrarse un aumento de 12 a 13 hosts con vulnerabilidades identificadas respecto al período anterior. En total, se detectaron 15 vulnerabilidades, distribuidas en 12 de severidad media y 3 de severidad baja, lo que sitúa la métrica general de vulnerabilidades en un 7%. Aunque este porcentaje refleja una postura de riesgo moderada y un nivel de exposición relativamente controlado, el incremento en la cantidad de activos afectados evidencia la necesidad de reforzar las actividades de gestión de vulnerabilidades. En este contexto, se recomienda priorizar la remediación de las vulnerabilidades de severidad media, complementar estas acciones con evaluaciones periódicas de seguridad y mantener un monitoreo continuo de los activos expuestos. Estas medidas contribuirán a reducir la superficie de ataque, fortalecer la postura de ciberseguridad de la organización y disminuir la probabilidad de explotación de vulnerabilidades por parte de actores maliciosos.

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