TLP:AMBER

BOARDROOM EXECUTIVE REPORT

TROPIGAS

September 02, 2026

TROPIGAS 09/02/2026

TLP AMBER BOARDROOM

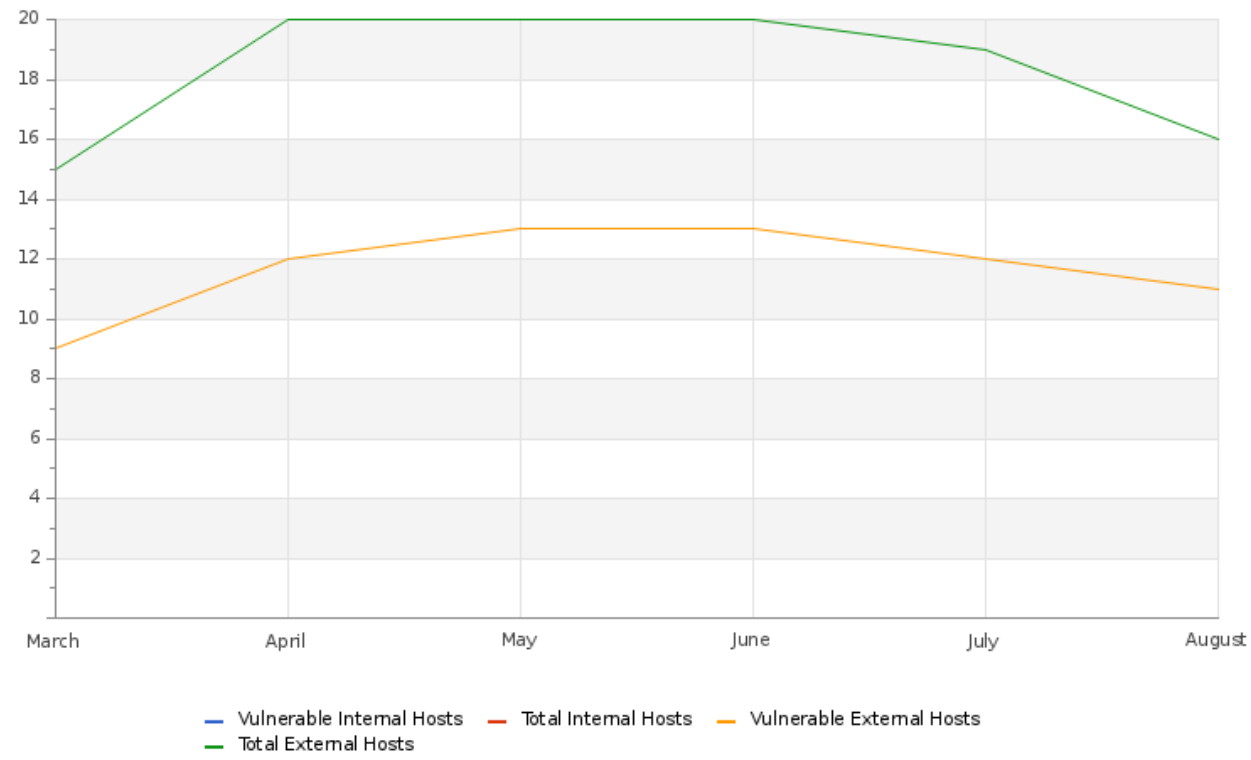
EXECUTIVE REPORT

Este informe corresponde "AGOSTO 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 los últimos meses, la métrica muestra la evolución de los sistemas externos identificados y de los hosts con vulnerabilidades. Entre julio y agosto, los sistemas identificados pasaron de 19 a 16, mientras que los hosts con vulnerabilidades pasaron de 12 a 11. Para agosto, 11 de los 16 sistemas identificados presentaron vulnerabilidades. La comparación refleja una disminución en la cantidad de sistemas expuestos y una ligera reducción en los hosts con vulnerabilidades respecto al período anterior. Se recomienda mantener el seguimiento continuo de los activos expuestos y continuar con las acciones de remediación sobre las vulnerabilidades identificadas.

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

TROPIGAS 09/02/2026

Total Attacks Successfully Blocked

37346306

Durante el mes de agosto se registraron 545,594 ataques bloqueados, frente a 6,028,677 registrados en julio, lo que representa una disminución aproximada del 90.95 %. Esta reducción estuvo principalmente influenciada por la disminución de eventos asociados a Information Leakage respecto al período anterior.

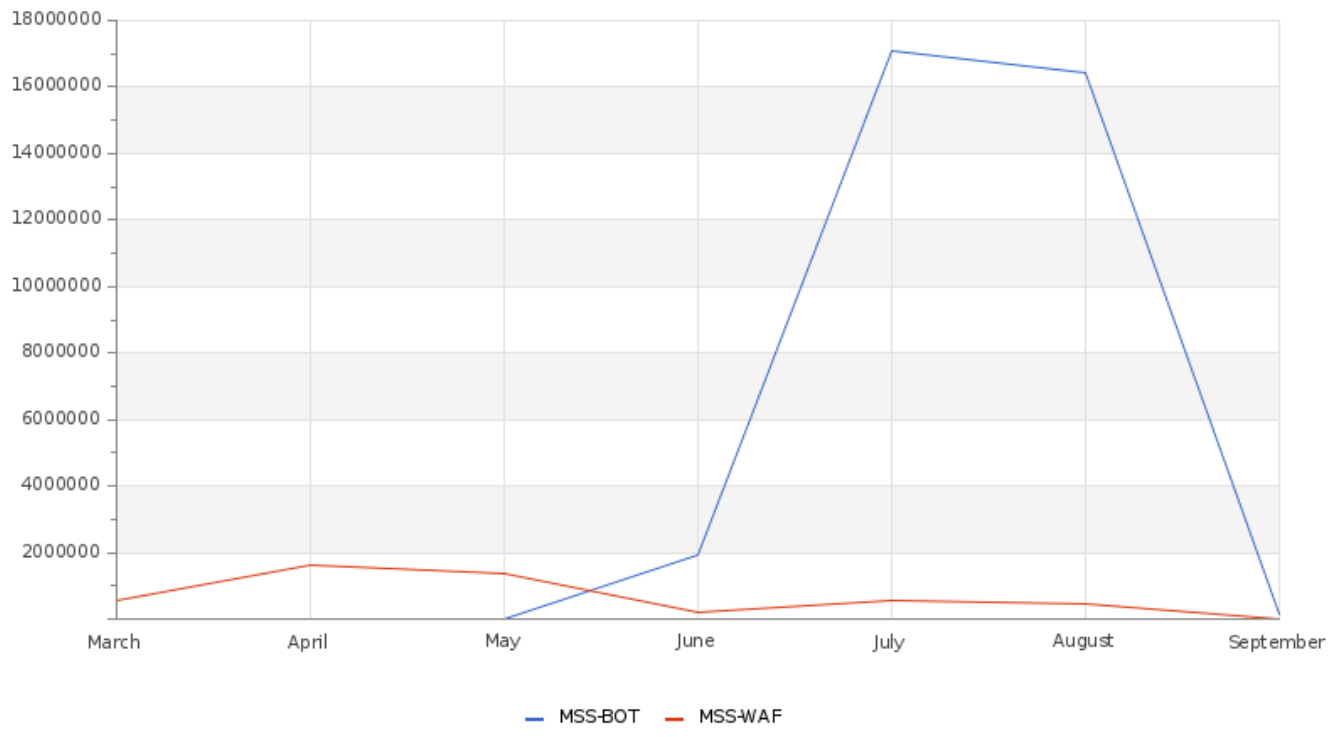
Critical Attacks Successfully Blocked

1210458

Durante el mes de agosto se registraron 469,845 ataques críticos bloqueados, frente a 591,415 registrados en julio, lo que representa una disminución aproximada del 20.58 %. A pesar de la reducción, los eventos críticos representaron el 86.11 % del total de ataques registrados durante agosto.

TROPIGAS 09/02/2026

Attacks Successfully Blocked



Durante el mes de agosto se registraron 545,594 ataques bloqueados por MSS-WAF CLOUD, frente a 6,028,677 registrados en julio, lo que representa una disminución aproximada del 90.95 %. Por su parte, se registraron 16,422,735 eventos asociados a BOT, frente a 17,641,812 registrados en julio, representando una disminución aproximada del 6.9 %. La actividad observada corresponde a eventos identificados y bloqueados por los controles MSS-WAF y MSS-BOT, que permitieron gestionar solicitudes maliciosas y tráfico automatizado dirigido contra las aplicaciones y servicios protegidos. A pesar de la disminución en ambos tipos de eventos, los mecanismos de seguridad continuaron operando de manera efectiva durante agosto para identificar y bloquear la actividad detectada.

Vulnerability Metric

8

Para el período de agosto de 2026, el análisis de la superficie externa identificó 16 sistemas expuestos a Internet, de los cuales 11 presentan vulnerabilidades activas, con un total de 25 vulnerabilidades: 17 de severidad media y 8 de severidad baja, sin hallazgos críticos ni altos. Las principales debilidades identificadas durante el período están relacionadas con configuraciones de seguridad web y mecanismos criptográficos, incluyendo ausencia de HSTS, uso de protocolos TLS obsoletos como TLS 1.1, certificados SSL autofirmados, no confiables o próximos a expirar, así como soporte de suites criptográficas asociadas a SWEET32 y divulgación de información de Microsoft Exchange. Los resultados de agosto muestran una reducción en la cantidad de sistemas expuestos y vulnerabilidades activas respecto al período anterior, aunque persisten oportunidades de fortalecimiento principalmente en las configuraciones SSL/TLS, cabeceras de seguridad y divulgación de información. Por lo anterior, se recomienda mantener el seguimiento continuo de los activos expuestos y las acciones de remediación sobre los hallazgos identificados, priorizando aquellos que puedan incrementar la exposición del entorno.

TROPIGAS 09/02/2026

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