



GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

BOARDROOM EXECUTIVE REPORT

TROPIGAS
August 20, 2026



TROPIGAS 08/20/2026

TLP AMBER BOARDROOM

EXECUTIVE REPORT

Este informe corresponde "JULIO 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 seis meses se observa una reducción reciente tanto en la cantidad de sistemas descubiertos como en los hosts con vulnerabilidades. Entre junio y julio, los sistemas descubiertos disminuyeron de aproximadamente 19 a 16, mientras que los hosts vulnerables pasaron de 12 a 11. Asimismo, la tendencia de vulnerabilidades muestra una disminución de las de severidad media, que pasaron de aproximadamente 55 en junio a 47 en julio, mientras que las de severidad baja se mantuvieron alrededor de 20 y no se observan vulnerabilidades de severidad alta. Esta evolución refleja una reducción de la exposición respecto al mes anterior; sin embargo, la permanencia de vulnerabilidades medias y bajas en los activos identificados requiere mantener las acciones de remediación y seguimiento para continuar disminuyendo la superficie de ataque.

Total Attacks Successfully Blocked

13567718

Durante el mes de julio se registraron 6,028,677 ataques bloqueados, frente a 2,483,937 registrados en junio, lo que representa un incremento aproximado del 142.7 %. Este comportamiento refleja un aumento considerable en el volumen de actividad maliciosa dirigida contra los activos y servicios de la organización. A pesar del incremento observado, los controles de seguridad implementados lograron bloquear la actividad identificada, reduciendo la exposición de los recursos protegidos ante los diferentes vectores de ataque. Es importante señalar que el valor de 13,567,718 ataques bloqueados corresponde al acumulado de los últimos 90 días, por lo que no representa exclusivamente la actividad registrada durante julio.



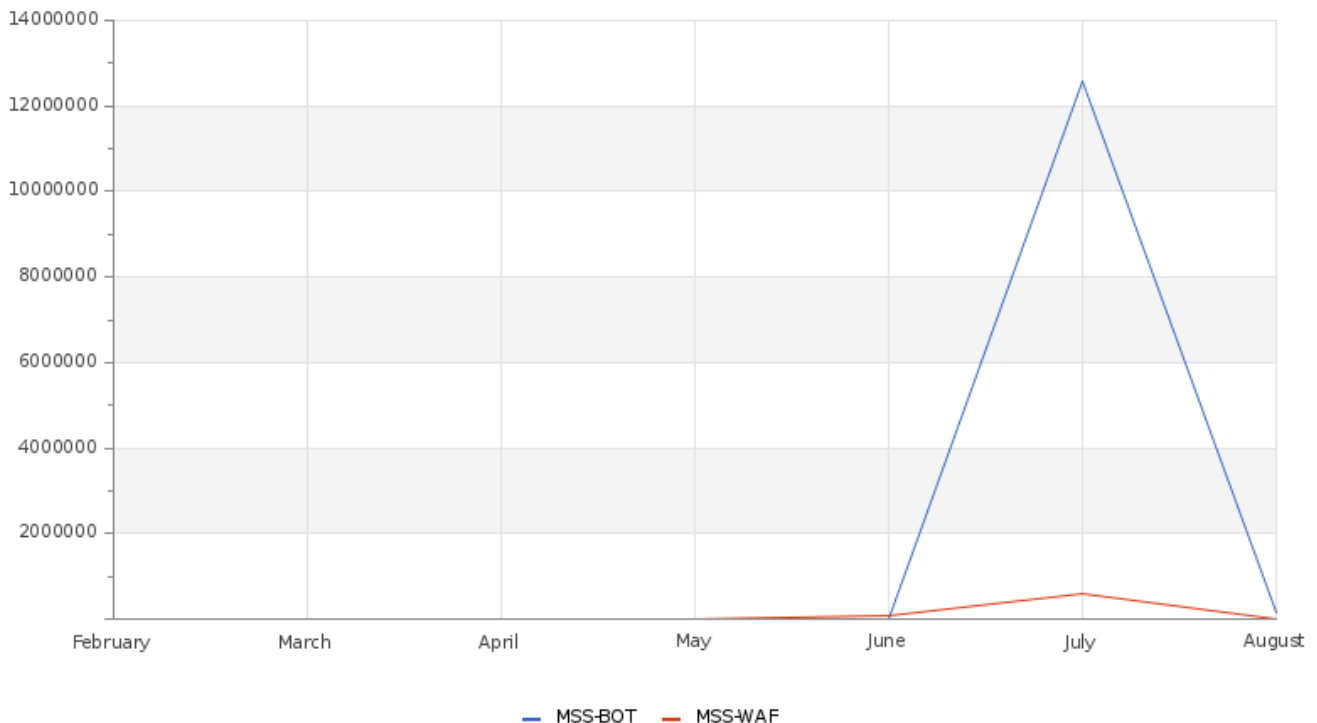
TROPIGAS 08/20/2026

Critical Attacks Successfully Blocked

664779

Durante el mes de julio se registraron 591,415 ataques críticos bloqueados, frente a 66,936 registrados en junio, representando un incremento aproximado del 783.5 %. Adicionalmente, los eventos críticos pasaron de representar aproximadamente el 2.69 % del total de ataques en junio al 9.81 % en julio, evidenciando no solo un incremento en el volumen de actividad, sino también una mayor concentración de ataques clasificados con nivel de riesgo crítico. Los controles de seguridad lograron bloquear estos eventos, evitando que la actividad identificada alcanzara los activos y servicios protegidos. De igual forma, el valor de 664,779 ataques críticos bloqueados corresponde al acumulados de mas de 30 días.

Attacks Successfully Blocked



Durante el mes de julio se registraron 6,028,677 ataques bloqueados, frente a 2,483,937 registrados en junio, lo que representa un incremento aproximado del 142.7 %. La actividad observada estuvo asociada a los controles de MSS-BOT y MSS-WAF, que permitieron identificar y bloquear solicitudes maliciosas y tráfico automatizado dirigido contra las aplicaciones y servicios protegidos. Este incremento evidencia una mayor actividad durante julio; sin embargo, los mecanismos de seguridad lograron contener los eventos identificados. Es importante señalar que los valores superiores mostrados en algunos indicadores corresponden a acumulados de períodos más amplios, por lo que el total utilizado para el análisis mensual de julio es de 6,028,677 ataques bloqueados.

TROPIGAS 08/20/2026

Vulnerability Metric

5

El análisis de la superficie externa identificó 19 sistemas expuestos a Internet, de los cuales 12 presentan vulnerabilidades activas, con un total de 30 vulnerabilidades: 22 de severidad media y 8 bajas, sin hallazgos críticos ni altos. Las principales debilidades están relacionadas con configuraciones de seguridad web y mecanismos criptográficos, incluyendo ausencia de HSTS, uso de TLS 1.0, certificados SSL no confiables o próximos a expirar, soporte de suites criptográficas asociadas a SWEET32, así como exposición de archivos de respaldo y divulgación de información de Microsoft Exchange. Aunque individualmente estos hallazgos no representan una criticidad elevada, su combinación puede ampliar la superficie de ataque y proporcionar información útil para actividades de reconocimiento o posteriores intentos de explotación, por lo que se recomienda fortalecer las configuraciones SSL/TLS, aplicar cabeceras de seguridad y restringir la exposición innecesaria de recursos e información.

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.**





GLE
SEC

COMPLETELY
PERCEPTIVE

TLP:AMBER

BOARDROOM EXECUTIVE REPORT

HOW CAN WE HELP?

Contact us today for more information on
our services and security solutions.

