TLP:AMBER

CISO EXECUTIVE REPORT

ORGANO JUDICIAL

July 19, 2023

Organo Judicial 07/19/2023

TLP AMBER CISO

EXECUTIVE REPORT

Este informe corresponde a junio 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.

ABOUT THIS REPORT

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.

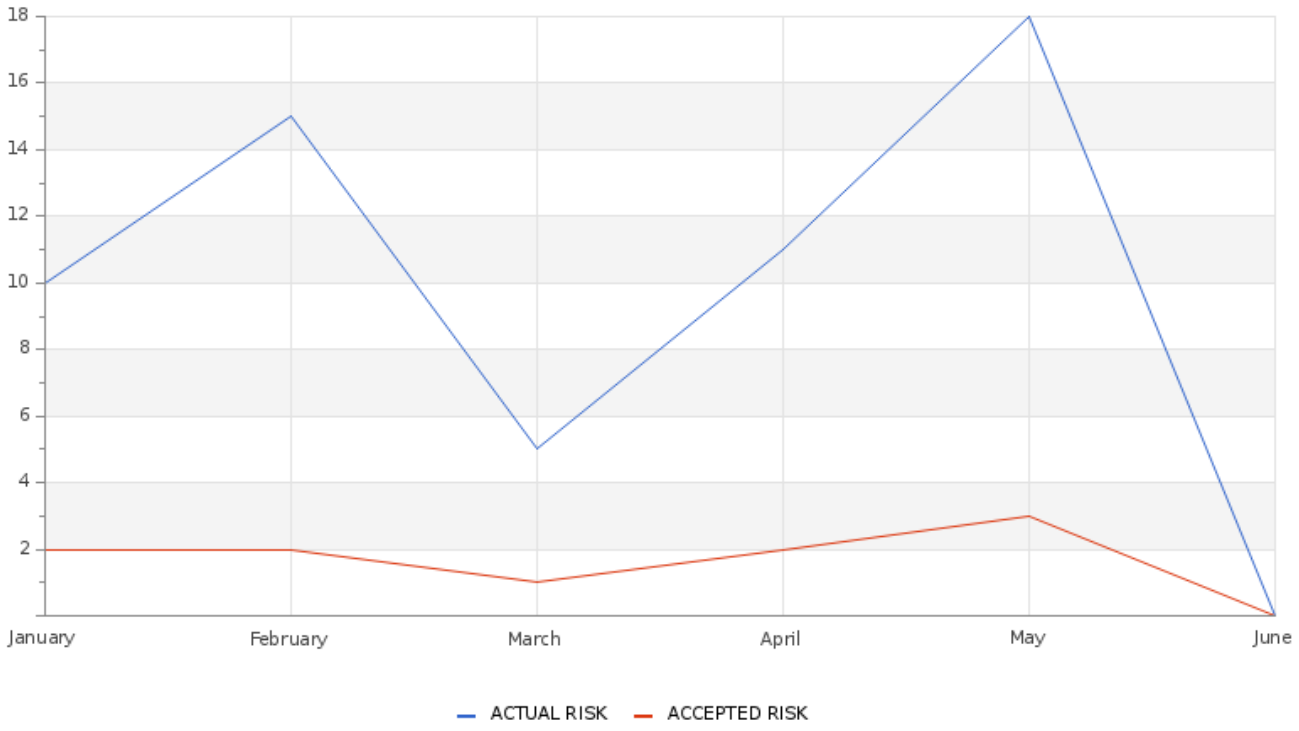
RISK

Actual Risk	Accepted Risk	Confidence
0%	0%	Low

Accepted & Actual Risk

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

Organo Judicial 07/19/2023

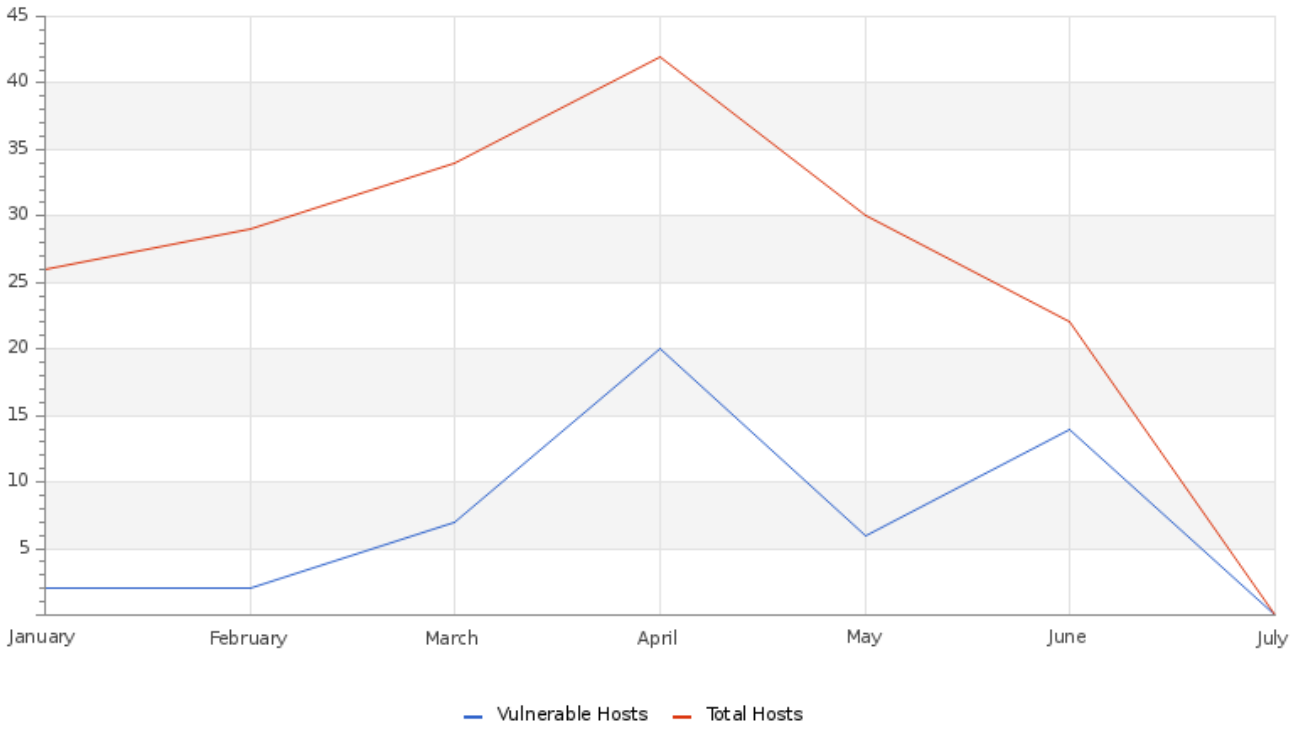


El nivel de riesgo actual es critico, debido a que hay servidores que son vulnerables y estos reciben ataques que se correlacionan con el servicio MSS-DDOS, toda esta información esta detallada en nuestra plataforma SKYWATCH.

VULNERABILITY

Organo Judicial 07/19/2023

Hosts & Vulnerable Hosts In Last 6 Months



Se puede observar que las vulnerabilidades descubiertas han incrementado en los últimos meses, muchas de estas están relacionadas a actualizaciones. Se recomienda dar solución y así mejorar las postura de seguridad de su empresa o organización.
Para este período el número total de vulnerabilidades se clasifica en: 19 para el riesgo crítico, 41 para el riesgo alto, 125 para el riesgo medio y 12 para el riesgo bajo.

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

Organo Judicial 07/19/2023

Total Vulnerability Counts In Current & Previous Month

	Current Month	Previous Month
Hosts Baselined	38	35
Hosts Discovered	21	13
Vulnerable Hosts	13	2
Critical Vulnerabilities Count	19	0
High Vulnerabilities Count	41	0
Medium Vulnerabilities Count	121	10
Low Vulnerabilities Count	10	2
Phishing Score	0	0
Email Gateway Score	1	1
Web Application Firewall Score	0	0
Web Gateway Score	54	58
Endpoint Score	5	2
Hopper Score	0	0
DLP Score	0	0

Recomendamos ajustar su política de archivos contra la lista de permitidos y bloqueados informados en BAS Web Gateway Vector para disminuir su superficie de ataque. En relación al servicio MSS-BAS Amenazas inmediatas, muchas de estas amenazas han eludido sus contramedidas de seguridad en EDR, Email y web Gateway/browser. Consulté nuestra plataforma para ms detalles.

Vulnerability Metric

65

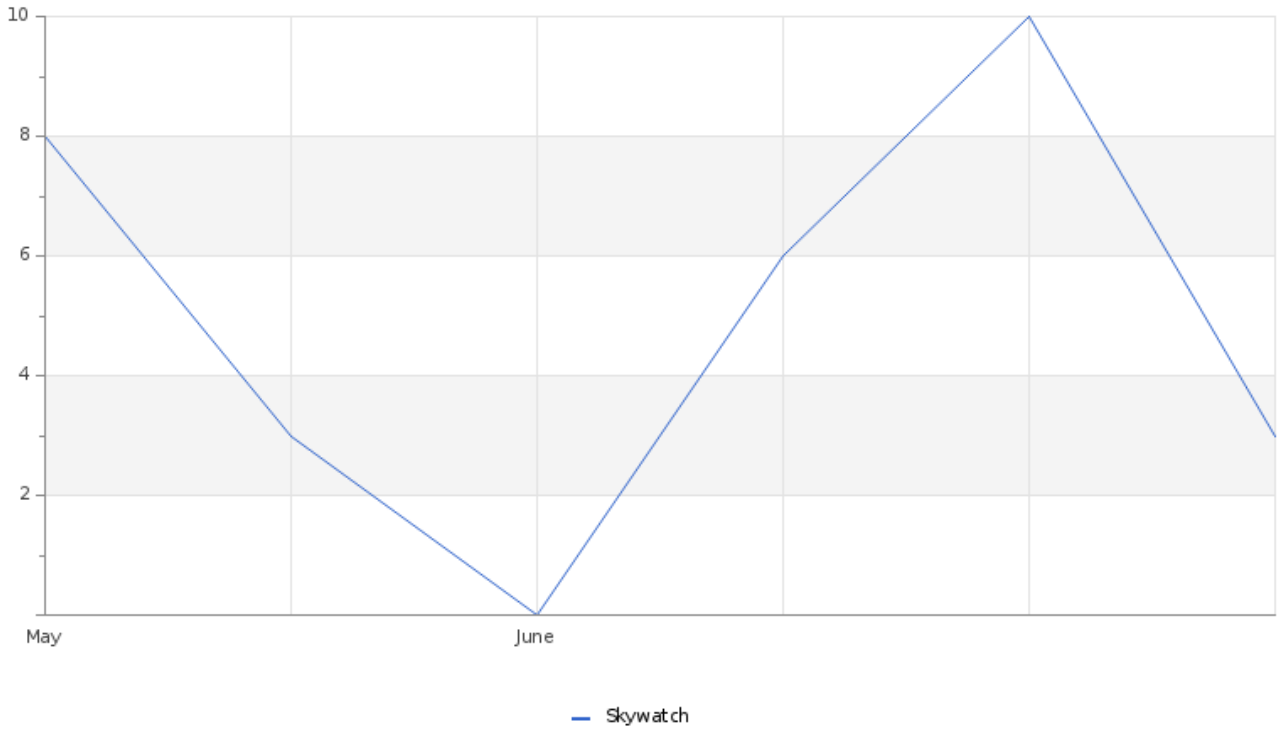
Hemos identificado y recomendado acciones para abordar y mitigar las vulnerabilidades a nivel externo. La información está bien documentada en la utilidad C&RU de SKYWATCH.

THREATS

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

Organo Judicial 07/19/2023

Total Number of Successful MFA authentications per application

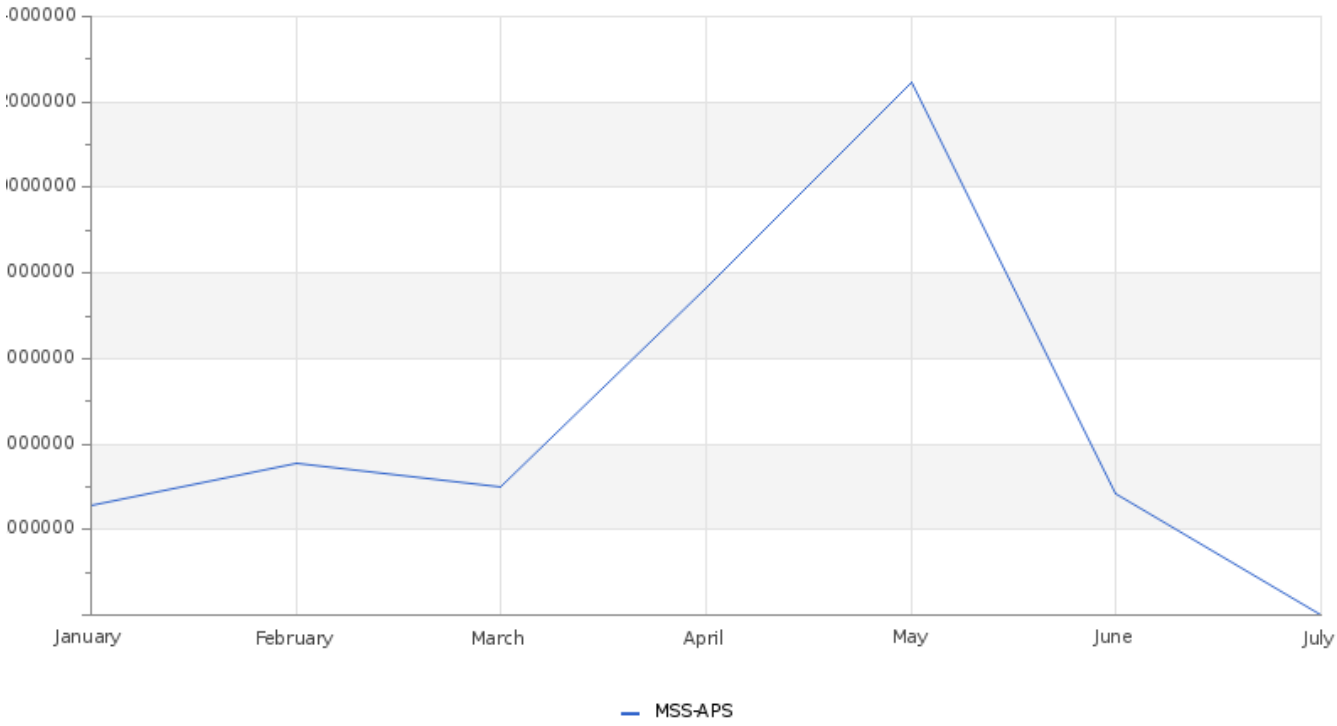


Nuestros registro muestran contantemente actividad por parte de los usuarios que usan la plataforma SKYWATCH, esto a fin de seguir las recomendaciones, incidentes, reportes, etc,que nuestro SOC ha estado monitoreando 24/7.

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

Organo Judicial 07/19/2023

Total Attacks Successfully Blocked Per Service

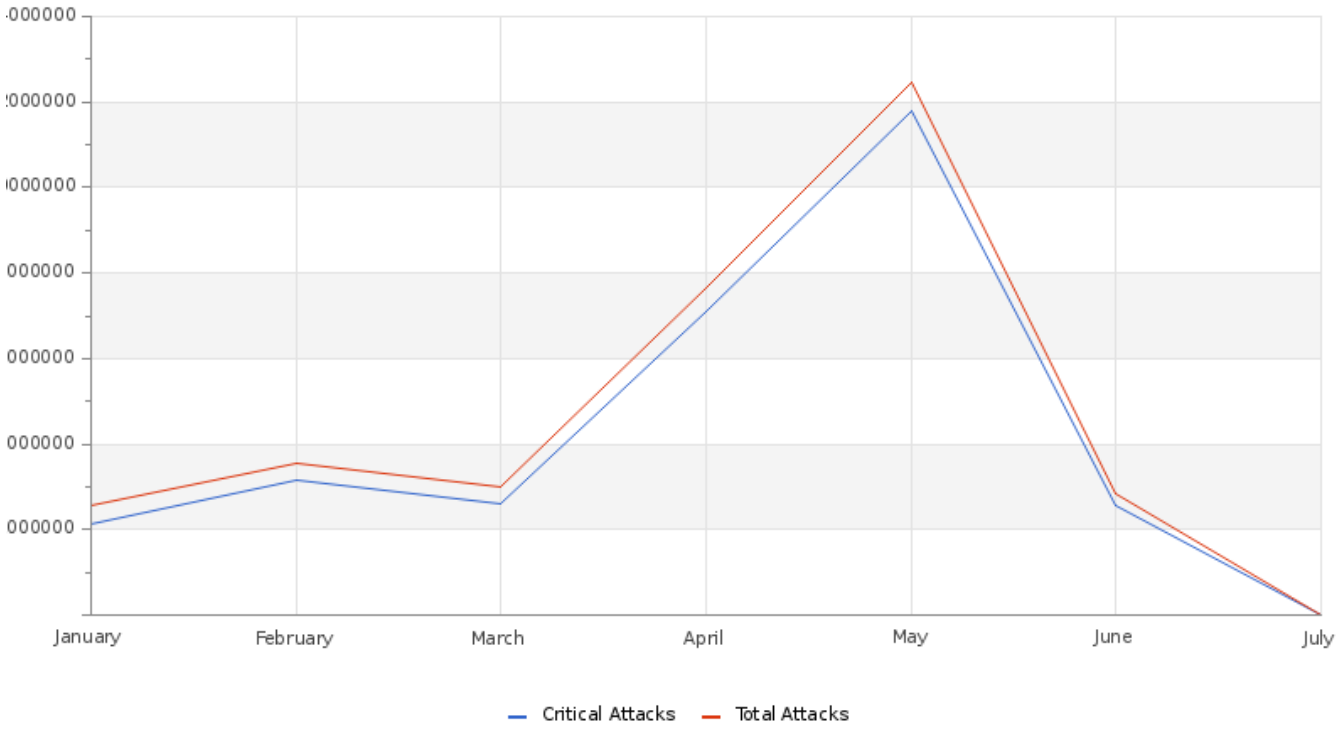


Durante el periodo del se han recibido 2,894,066 ataques totales, en nuestro monitoreo hemos investigado y abierto casos de persistencia las cuales hemos notificado al personal encargado. La gran mayoría de ataques provienen de IPs maliciosas/Botnets, ataques ErtFeed y GeoFeed.

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

Organo Judicial 07/19/2023

Attacks Successfully Blocked by Severity



El número de ataques críticos fue de 2,632,224,los tipos de ataque más persistente es el de Ertfeed, éste se centra en una inteligencia única en tiempo real que puede proporcionar protección preventiva contra amenazas emergentes específicas de DDoS, incluido IoT en evolución botnets y nuevos vectores de ataque DNS.

System Availability and Performance in current & previous month

	Current Month	Previous Month
Total Down Devices	4	1
Critical Down Devices	0	0

Histogram of Total and Critical Device Outages

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

Organo Judicial 07/19/2023

OPERATIONAL

Notable Events Active For The Last Month

Notable Event Type	How Many #
BAS Immediate Threat	36
Change in Critical Perimeter Attacks	8
BAS Web Security	18
Change in High or Critical Vulnerabilities	7
Change in Baseline Systems Discovered	2
Change in Systems Availability	1

Durante el periodo del mes se han abiertos casos de vulnerabilidad, casos de persistencia e investigaciones que personal de Organo Judicial ha solicitado en el servicio MSS-DDOS, también se han documentados los casos del servicio MSS-BAS, los cuales se recomienda revisarlos y aplicar las soluciones ya que muchos de estos están relacionados a amenazas inmediatas, para más información puede acceder a nuestra plataforma para clientes https://skywatch.glesec.com en la sección CR&U.

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

CISO 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