

|                                 |                                   |
|---------------------------------|-----------------------------------|
| Alerta de seguridad cibernética | 4IIA23-00067-01                   |
| Clase de alerta                 | Intentos de Intrusión             |
| Tipo de incidente               | Intentos de acceso – Fuerza bruta |
| Nivel de riesgo                 | Alto                              |
| TLP                             | Blanco                            |
| Fecha de lanzamiento original   | 09 de junio de 2023               |
| Última revisión                 | 09 de junio de 2023               |

## NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del equipo CSIRT. La información contenida en los informes o comunicados está afecta a actualizaciones, por lo cual se recomienda establecer una cuarentena preventiva respecto de los loC mencionados, previa evaluación de impacto en servicios productivos; una vez que sus plataformas de monitoreo no detecten actividad maliciosa, se debe evaluar la posibilidad de liberar del bloqueo a los loC consignados en el reporte respectivo, tales como servicios de hosting, de cloud o similares.

## Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT), ha identificado una serie de intentos de acceso a servidores de correos del sector público y privado. Estos ataques de fuerza bruta intentan vulnerar la autenticación del protocolo para transferencia simple de correos (SMTP) para suplantar a los remitentes originales y depositar correos con contenido o enlaces maliciosos en las bandejas de entrada de sus potenciales víctimas.

## Indicadores de compromiso

| IP             | Etiqueta de sistema autónomo | Nombre sistema autónomo |
|----------------|------------------------------|-------------------------|
| 80.94.95.242   | AS 204428                    | SS-Net                  |
| 45.66.230.176  | AS 211252                    | Delis LLC               |
| 107.182.128.12 | AS 399471                    | AS-SERVERION            |
| 194.85.249.206 | AS 399471                    | AS-SERVERION            |
| 185.252.179.55 | AS 46308                     | AS46308                 |
| 193.56.29.186  | AS 210228                    | Web Hosted Group Ltd    |

## Recomendaciones

- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Utilizar los registros SPF, DKIM y DMARC.
- Revisar o configurar correctamente los filtros de AntiSpam
- Revisar los controles de seguridad de los AntiSpam y SandBoxing.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras).
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.