

**Alerta de Seguridad Cibernética**

|  |  |
| --- | --- |
| **Alerta de seguridad cibernética** | 4IIA23-00063-01 |
| **Clase de alerta** | Intentos de Intrusión |
| **Tipo de incidente** | Intentos de acceso – Fuerza bruta |
| **Nivel de riesgo** | Alto |
| **TLP** | Blanco |
| **Fecha de lanzamiento original** | 27 de febrero de 2023 |
| **Última revisión** | 27 de febrero 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 IoC 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 IoC 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 para 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** |
| 80.94.95.205 | AS 204428 | SS-Net |
| 46.148.40.131 | AS 15828 | Blue Diamond Network Co., Ltd. |
| 46.148.40.24 | AS 15828 | Blue Diamond Network Co., Ltd. |
| 46.148.40.98 | AS 15828 | Blue Diamond Network Co., Ltd. |
| 46.148.40.177 | AS 15828 | Blue Diamond Network Co., Ltd. |
| 80.94.95.204 | AS 204428 | SS-Net |

**Recomendaciones**

* Evaluar el bloqueo preventivo de los indicadores de compromisos.
* Utilizar los registros SPF, DKIM y DMARCK
* 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.