Alerta de seguridad cibernética	4IIA21-00043-01
Clase de alerta	Intentos de Intrusión
Tipo de incidente	Intentos de acceso – Fuerza bruta
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	22 de septiembre de 2021
Última revisión	22 de septiembre de 2021

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 de Gobierno) 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 electrónicos con contenido o enlaces maliciosos en las bandejas de entrada de sus potenciales víctimas.

Indicadores de compromiso

N°	IP	Etiqueta de sistema autónomo
1	31.130.184.64	Blue Diamond Network Co., Ltd.
2	87.246.7.245	SS-Net
3	31.130.184.132	Blue Diamond Network Co., Ltd.
4	87.246.7.228	SS-Net
5	5.188.206.102	Krez 999 Eood
6	5.188.206.154	Krez 999 Eood
7	5.188.206.156	Krez 999 Eood
8	5.188.206.101	Krez 999 Eood
9	5.188.206.100	Krez 999 Eood
10	5.188.206.158	Krez 999 Eood
11	5.188.206.155	Krez 999 Eood
12	5.188.206.99	Krez 999 Eood
13	5.188.206.157	Krez 999 Eood
14	5.188.206.98	Krez 999 Eood
15	5.188.206.157	Krez 999 Eood
16	5.188.206.98	Krez 999 Eood

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.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.09.22 15:39:05 -03'00'