Alerta de seguridad cibernética	4IIA21-00039-01
Clase de alerta	Intentos de Intrusión
Tipo de incidente	Intentos de acceso – Fuerza bruta
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de junio de 2021
Última revisión	03 de junio 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 del Gobierno de Chile (CSIRT de Gobierno), ha identificado una serie de intentos de acceso a servidores de correo de los sectores público y privado. Estos ataques de fuerza bruta intentan vulnerar la autenticación del protocolo para transferencia simple de correos (SMTP), con el objetivo de 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 detectadas y activas

IP	Etiqueta de sistema autónomo
185.143.223.26	Technology Advanced Investment Limited
45.227.253.210	ru-informtech-1-mnt
78.128.113.109	DirectWebH CORP
185.24.233.143	Miti 2000 EOOD
185.24.233.142	ServeByte VPS
13.68.134.15	ServeByte VPS
103.155.80.188	Microsoft Corporation
91.191.209.234	VIET SPEED SERVICE COMPANY LIMITED
103.155.81.125	L&L Investment Ltd.
77.247.110.231	VIET SPEED SERVICE COMPANY LIMITED

IP reportadas en informes anteriores y que aún se encuentran activas hasta la fecha de este reporte:

5.188.206.182

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.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.06.03 22:42:27 -04'00'