**ALERTA DE SEGURIDAD DE LA INFORMACIÓN**
**RANSOMWARE EN SISTEMAS DEL**
**SERVICIO NACIONAL DE ADUANAS**
**TLP: BLANCO**

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) del Ministerio del Interior y Seguridad Pública informa a todos los organismos de la administración pública del descubrimiento de un ransomware conocido como Black Basta en una parte acotada de la infraestructura digital del Servicio Nacional de Aduanas.

Por esto, les recomendamos a todos los organismos realizar al menos las siguientes acciones preventivas:

- Verificar que las copias de seguridad se encuentren protegidas y en diferentes lugares.
- Monitorear los Active Directory; se recomienda auditar las cuentas de administración, reducir la cantidad de usuarios con permisos de administración, y chequear los siguientes:
    - Creación de cuentas con privilegios
    - Elevación de permisos no autorizados
    - Aparición de herramientas de escaneos
        - Netcat
        - PsExec
        - PowerShell
        - Rclone
- Revisar logs de antivirus o sistemas de protección por lo menos 15 días hacia atrás para identificar las amenazas que han sido bloqueadas.
- Revisar qué aplicaciones han sido ejecutadas en los servidores y estaciones de trabajo en el mismo rango de tiempo.
- Forzar un escaneo completo, desactivando la opción de solo analizar archivos nuevos.
- Verificar si existen conexiones a torrents
- Auditar su tráfico de red.
- Conservar un registro actualizado de sus sistemas para garantizar un monitoreo efectivo.
- Revisar la actividad de los eventos de Microsoft Windows (Active Directory) con los siguientes ID:
- Tareas programadas
    - 106: El usuario registró una nueva tarea programada
    - 4702: Se actualizó una tarea programada
    - 4699: Se eliminó una tarea programada

Servicios

- 4697: Se instaló un servicio en el sistema
- 7034: El servicio finalizó inesperadamente
- 7045: Se creó un nuevo servicio en la máquina local de Windows

Administración de cuentas

- 4720: Se creó una cuenta de usuario
- 4724: Se intentó restablecer la contraseña de una cuenta
- 4782: Acceso a hash de contraseña
- 4624: Se inició sesión correctamente en una cuenta
- 4625: Una cuenta no pudo iniciar sesión
- 4672: Privilegios especiales asignados al nuevo inicio de sesión
- 4634: Cierre de sesión exitoso
- 4776: Inicio de sesión fallido o exitoso a través de dominio

Red

- 5140: Se accedió a un objeto compartido de red
- 4778: Se volvió a conectar una sesión RDP
- 4104: Ejecución de PowerShell

Les pedimos asimismo que se mantengan al tanto de esta situación a través de los canales oficiales de información de Aduanas (http://www.aduana.cl/, https://twitter.com/AduanaCL) y del CSIRT (https://www.csirt.gob.cl/noticias, https://twitter.com/CSIRTGOB).

Finalmente, les recordamos que ante cualquier inquietud sobre esta información u otros requerimientos para detectar y mitigar vulnerabilidades o reportar un incidente, pueden contactar al CSIRT de Gobierno a través del correo electrónico incidentes@interior.gob.cl o llamar al 1510.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.10.17 12:26:17 -03'00'