ALERTA DE SEGURIDAD DE LA INFORMACIÓN
IOC RANSOMWARE EN EMPRESA DE TELECOMUNICACIONES
TLP: BLANCO

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) del Ministerio del Interior y Seguridad Pública fue notificado por la empresa GTD sobre un ransomware que afectó parte de sus plataformas IaaS durante la mañana del lunes 23 de octubre. Como consecuencia, algunos servicios públicos en nuestro país han presentado indisponibilidad en sus sitios web.

Por esta razón, de acuerdo a lo informado por la institución afectada, la empresa bajó sus plataformas IaaS para revisarlas de forma exhaustiva, analizar el incidente e impacto. **Le solicitamos a todas las instituciones públicas que tengan servicios IaaS contratados con GTD comunicar lo antes posible al CSIRT de Gobierno al correo incidentes@interior.gob.cl, según lo establece el decreto N° 273.**

GTD se encuentra trabajando con el CSIRT de Gobierno para entregar la información de forma oportuna, con el fin de implementar medidas de mitigación lo antes posible. Recomendamos a todas las instituciones que tienen servicios IaaS con GTD considerar las siguientes medidas de prevención:

- Realizar un escaneo completo a su infraestructura con antivirus.
- Verificar que no exista algún software sospechoso en sus sistemas.
- Revisar las cuentas existentes en su servidor y confirmar que no se hayan creado nuevas cuentas.
- Analizar el rendimiento de procesamiento y discos duros para asegurarse que no esté alterado.
- Revisar si hay algún tipo de variación en la información o fuga de datos de la empresa y sus bases de datos.
- Revisar su tráfico de red.
- Conservar un registro actualizado de sus sistemas para garantizar un monitoreo efectivo.
- Restringir el acceso a través de SSH a servidores, solo en caso estrictamente necesario.

Asimismo, gracias a una muestra compartida por GTD, en el CSIRT hallamos los siguientes IoC,

SHA256	Nombre Archivo	Descripción
58c20b0602b2e0e6822d415b5e8b53c348727d8e145b1c096a6e46812c0f0cbc	log.dll	Ransomware DLL
5822b7c0b07385299ce72788fd058ccadc5ba926e6e9d73e297c1320feebe33f	TmDbgLog.dll	Ransomware DLL
43a3fd549edbdf0acc6f00e5ceaa54c086ef048593bfbb9a5793f52a7cc57d1c	u.exe	Vector de ejecución (TrendMicro AirSupport)
3476f0e0a4bd9f438761d9111bccff7a7d71afdc310f225bfebfb223e58731e6	d.exe	Vector de ejecución (BitDefender Update Downloader)

Cabe destacar que los programas u.exe y d.exe detectados en las máquinas infectadas son aplicaciones legítimas de distintos antivirus. Sin embargo, el atacante aprovecha vulnerabilidades existentes en ellas para la carga lateral de las DLL maliciosas. El atacante sube a la máquina a infectar ambos archivos ejecutables, por lo que no es necesario que la máquina afectada posea estos programas instalados en ella.

Les recordamos la importancia de contar con usuarios con el mínimo de privilegios y realizar copias de seguridad de forma regular, almacenándolas en diferentes lugares y medios.

Finalmente, pueden escribir al CSIRT de Gobierno al correo electrónico incidentes@interior.gob.cl, o llamar al 1510.

CSIRT
Gobierno de
Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.10.24 17:04:04 -03'00'