Cercano al día viernes 9 de octubre, se dio a conocer un ciberataque que afectó a la división de Gobierno Digital. Este hecho fue denunciado por los mismos ciberdelincuentes mediante un defacement al sitio web digital.gob.cl, informando que habían accedido a los sistemas y que tenían en su poder mucha información relacionada con el gobierno y con ciudadanos.

Posteriormente, mediante la cuenta de twitter “@elturista_1”, se comenzó a divulgar poco a poco la información que se había sustraído desde los servidores de Gobierno Digital.

Los archivos divulgados corresponden a códigos fuente, dump de bases de datos, archivos de configuración y archivos de sistema, entre otros.

Gobierno Digital, durante los últimos 5 años, ha impulsado fuertemente la transformación digital de las instituciones de gobierno, desarrollando plataformas y sistema que permiten simplificar y digitalizar trámites que por lo general se realizaban de forma presencial. Por este motivo, muchas instituciones de gobierno utilizan las plataformas y sistemas de Gobierno Digital, la cual fue víctima de un ciberataque estos últimos días el cual afectó, de forma indirecta, a todas estas instituciones que dependen de las plataformas de Gobierno Digital.

El equipo de investigación de NIVEL4 se dedicó a revisar los documentos expuestos con el fin de poder determinar el impacto real de este incidente, identificando instituciones y organismos que fueron afectados como también información técnica, sensible y personal comprometida.

Hemos logrado determinar que los siguientes sistemas o instituciones han sido afectados por este ciberataque:

- Registro Civil
- Carabineros (comisaría virtual)
- Servicio Médico Legal (SML)
- Dirección General de Aguas (DGA)
- Registro Nacional de Trámites (Min SegPres)
- Sistema de Trámites Online de Extranjería
- ChileAtiende / IPS
- Sistema “CeroFilas”

Los sistemas en la nube y locales, han sido puestos en riesgo mediante la divulgación de tokens y claves, como por ejemplo:

- Acceso a Buckets de AWS con información sensible
- API-KEY para consultar servicios que no son públicos ni abiertos
- Token para consumir recursos externos
- Token de sesión
- Certificados digitales y llaves privadas
- Credenciales de acceso a sistemas web

Producto del ciberataque y posterior divulgación de archivos, se puso en riesgo todas las “interconexiones” que tienen los sistemas, ya que se divulgaron certificados, llaves privadas, token de accesos, api keys, usuarios, contraseñas, etc.

Adicionalmente, se divulgó información personal sobre funcionarios públicos quienes operan las plataformas como los ciudadanos que hacen uso de las

plataformas, incluyendo números de serie de cédulas de identidad, número de pasaporte y documentos de identificación escaneados.

El análisis realizado por el equipo de investigación de NIVEL4, ha logrado detectar hasta el momento, cuentas de usuario y credenciales de más de 5 millones de usuarios. A modo de ejemplo, se contabilizó los registros de las tablas “usuario” correspondientes a las bases de datos de Carabineros, Extranjería y Chile Atiende:

Institución	**Cantidad de Usuarios**
Carabineros	1.405.218
Extranjería	6.579.274
Chile Atiende / IPS	542
Total	**7.985.034**

Se debe considerar que hay más de 10GB de información.

Debido a esto, el incidente es de carácter crítico y es necesario una pronta respuesta por parte de los afectados.

Como NIVEL4, recomendamos que la institución responsable emita un comunicado oficial a las entidades afectadas, con el fin de que puedan tomar las acciones correspondientes. Se debe realizar una revisión de todos los sistemas que se interconectan con las plataformas de gobierno digital y cambiar los token de accesos o credenciales, según corresponda. Adicionalmente, recomendamos identificar a las personas afectadas y evaluar el impacto que pueda tener la divulgación de sus datos o acceso a sistemas personales e institucionales.

Ninguna institución o empresa está exenta de un ciberataque, sin embargo, podemos trabajar en prepararnos para disminuir las posibilidades de sufrir uno mediante la detección continua de vulnerabilidades y amenazas. También podemos trabajar en gestionar un incidente de manera correcta en caso que este se materialice, ya sea técnicamente como mediáticamente.