ALERTA DE SEGURIDAD CIBERNÉTICA
CAMPAÑA DE MALWARE EN ENTIDAD PÚBLICA

El Equipo de Respuesta ante Incidentes de Seguridad Informática del Gobierno de Chile, CSIRT de Gobierno, informa que esta mañana fue detectado un malware de tipo *infostealer* que llegó a través de un correo electrónico en una organización del Estado.

El malware fue identificado como URSA/Mispadu, del grupo de amenaza Malteiro, el cual concentra su actividad maliciosa especialmente en Iberoamérica.

La entidad que detectó la actividad maliciosa indicó que el malware fue descargado en un PC, pero éste fue contenido por el EDR y no habría logrado comprometer los activos asociados al dispositivo.

Este malware/infostealer no es detectado oportunamente por todos los antivirus comerciales. En consecuencia, sugerimos a los administradores de seguridad TI poner atención a los siguientes indicadores de compromiso y recomendamos aplicar cuarentenas sobre estos:

- ~~ [7d71b59da9115756d6f23a77e9b5841f624c71bf4cb3556fbc246720c0fb171d]
- ~~ [bbfd049f7c42a43248f9c6fae52640938b6343b3761f26db77c82ad0cd6394d4]
- DriverAudio.lnk [da788c5a5ea8ef856f59954043b9a2db3b02269cb21fbd1af20ef4eb7c616046]
- Factura_Deuda_423534.a3x [dedf8d748b672a1b689405ea0369da4a77c7de8acf839b1422888984e9915fca]
- jordan.exe [98e4f904f7de1644e519d09371b8afcbbf40ff3bd56d76ce4df48479a4ab884b]

Adicionalmente, compartimos otros indicadores de compromiso relacionados al incidente y solicitamos analizar y evaluar la aplicación de cuarentenas preventivas en los casos que corresponda:

- http://www.sxconstructions.com[.]au/wp-content/img/do/it.php?b1&v1=1033&v2=1033&v3=&v4=Windows%207&v5=User&v6=X86&v7=
- http://germogenborya[.]top/rest/?h=C4BA3647
- 173.254.29[.]24
- 85.193.93[.]125, esta IP están relacionadas con:
  - portaconexao8[.]top
  - germogenborya[.]top
  - russianmen75[.]top

El CSIRT de Gobierno destaca la rápida reacción y eficiente manejo del incidente por parte de la entidad afectada, así como su disposición a compartir los indicadores de compromiso.

Complementariamente, queremos recomendar a las organizaciones de la Red de Conectividad del Estado, de la Administración Pública y entidades en convenio de colaboración, así como a las organizaciones privadas que reciban este documento, para que consideren las siguientes recomendaciones para fortalecer su ciberseguridad:

- Fomentar buenas prácticas y campañas de concientización de ciberseguridad entre los usuarios de sus organizaciones, especialmente en torno a la prevención frente a la amenaza del phishing.
- 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).
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet.
- Prestar atención en los detalles de los mensajes o redes sociales.
- Evaluar el bloqueo preventivo de los indicadores de compromisos.
- Mantener actualizadas todas las plataformas de tecnologías y de detección de amenazas.
- Revisar los controles de seguridad de los AntiSpam y SandBoxing.
- Realizar concientización permanente para los usuarios sobre este tipo de amenazas.
- Visualizar los sitios web que se ingresen sean los oficiales.
- Mantener actualizado sus sistemas operativos y aplicativos.

Si las organizaciones de las Red de Conectividad del Estado y de la Administración Pública en general detectan alguna anomalía en relación con las medidas de prevención indicadas en este documento, pueden comunicarse con el CSIRT de gobierno al correo soc@interior.gob.cl o al teléfono 1510, ambos disponibles en modalidad 24/7.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2023.02.08 23:07:20 -03'00'