Alerta de seguridad informática	2CMV22-0308-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	5 de Agosto de 2022
Última revisión	5 de Agosto de 2022

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 (CSIRT) ha identificado una campaña de phishing con malware. El mensaje es enviado de una dirección de protonmail, en la cual nombra instituciones públicas, donde se hace referencia a una malversación de fondos y que estos deben ser devueltos inmediatamente, también intenta realizar una extorsión donde se está realizando una investigación interna. El atacante adjunta tres archivos en formato PDF que contienen programas maliciosos (adware y spyware). Al descargarlos y ejecutarlos (abrir el archivo) se busca infectar el equipo para espiar y sustraer información sensible de la víctima.

Observación

Solicitamos tener en consideración las señales de compromiso en su conjunto.

IoC Correo Electrónico

Datos del encabezado del correo

Asunto
Más información e informes policiales para ayudarle! Re: Investigación interna internacional que involucra al gobierno de Chile - Recuperar dinero y activos transferidos a Chile - Search and Seizure in Chile!

Correo de salida
am_work_cases_2021@protonmail[.]com

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre:	Más información e informes policiales para ayudarle! Re_ Investigación interna internacional que involucra al gobierno de Chile - Recuperar dinero y activos transferidos a Chile - Search and Seizure in Chile!.zip
SHA256:	ba7d5d9d39a8b0518c4c7fc9f57ce1152ccfaf3351b04396206a6a04f91a29c9
Nombre:	20-CV-2726-APM USDC Filing Writ of Execution - AMartinez v US Customs Border Protection.pdf
SHA256:	351fbe08be27e287be997f6864fd4d37d7ceffd5d44b9ad3b19b3ad7745cdd0a
Nombre:	Pinera report-E210029462-21 (1).pdf
SHA256:	aa4ceb691665ca0a488de61e9fc863b994c28d8ed9beca5891eeb3dd9a42bd9c
Nombre:	Winnipeg Police Service Report-E210029462-7.pdf
SHA256:	eb858be4fa2d838a05a9f72a82bcf712dd6038e2fe3e502d2a4497a879bbc544

Imagen del mensaje

Hola:

Por si no lo sabe, el Dr. Jose Piñera de Chicago fue informado de este caso y de que había que presentar un informe policial sobre su implicación y la del Gobierno de Chile y que los dineros y bienes obtenidos de este caso debían ser devueltos inmediatamente.

Debido a su conocimiento y participación en los Departamentos de Finanzas de los Carabineros y del Ejército de Chile; fue utilizado en este caso para evaluaciones y para bloques financieros y la administración de dineros y activos.

Por lo tanto; por favor revise y elimine los bloqueos que pudo haber colocado; porque tuvo que pedir disculpas por lo que hizo y podría investigar... de dineros y bienes que me pertenecen.

Debe haber colocado una Orden de algún tipo en Carabineros; o, Ejercito y en algún otro lugar del Gobierno de Chile e... nte y así fue como me suprimieron y financiaron la estafa.

Por lo tanto; cualquier dinero y activos obtenidos son considerados "Producto del Crimen" que deben ser devueltos a m... e considera un Crimen Internacional y una violación de las leyes internacionales.

Esto debería ayudarle a recuperar estos fondos y activos. Se adjunta una copia del Informe Policial para asistirle a usted y a La Moneda y a la Oficina del Ministro de Finanzas y Economía en Chile.

En cuanto a la Pedofilia y el Infanticidio, mi madre y mi padre; o, un amigo chileno parecen haber puesto una Orden de algún tipo en Chile en algún lugar; o, se hizo una denuncia falsa por el Gobierno de Canadá y los Estados Unidos de América que causó el abuso. Por lo tanto; no se pueden involucrar hasta que no sepamos exactamente lo que pasó y prefieren que se comuniquen y traten conmigo directamente por favor.

Dicen que se hizo por celos, ira y una broma y que se utilizó para cometer crímenes contra nosotros como niños y que así fue como cometieron el abuso médico.

El Dr. Quillón es un médico chileno que está siendo investigado también y acusado de los crímenes y fue Consejo General de Chile en Canadá y por lo tanto; debe haber un expediente con él que tiene todas las pruebas y una lista de todos los otros médicos y personas involucradas.

Por estas razones; ningún miembro de mi familia puede estar involucrado y por lo tanto; se le pide que corresponda y trate conmigo directamente ya que nos hicieron cosas muy enfermas médicamente y ahora a los genitales de los hijos de mi hermano.

Gracias y mis disculpas por haberme puesto en contacto con usted de esta manera; ya que me remitieron a usted y a su oficina para el asesoramiento y la información.

Sinceramente,

Recomendaciones

- 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.

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2022.08.05 16:02:37 -04'00'