Alerta de seguridad cibernética	8FPH22-00537-01
Clase de alerta	Fraude
Tipo de incidente	Phishing WhatsApp
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	03 de junio de 2022
Última revisión	03 de junio de 2022

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del 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.

Estos casos de phishing no involucran directamente a las entidades ni al sistema bancario, sino que son técnicas de fraude indirecto, en las que en infraestructura externa a éstas se arma el mencionado phishing, para construir el engaño. Las entidades, en general, al tomar conocimiento de estos portales maliciosos articulan, dentro de sus potestades y marco legal vigente, las acciones necesarias para poder desarticularlos, pero ciertamente los usuarios también estamos llamados a estar atentos a estos intentos de engaño.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno), ha identificado una campaña de Phishing vía mensaje WhatsApp, que se hace pasar como proveniente de la empresa CGE.

En esta campaña, los delincuentes indican falsamente a la víctima que “CGE Energía ¡Subsidios energéticos del Gobierno!” Al ingresar al enlace, la persona es direccionada a un sitio semejante al de CGE, dónde se le invita a completar una falsa encuesta y participar en el sorteo. Al concluir las preguntas, aparece un supuesto proceso de verificación y se le solicita a la víctima participar en un falso juego donde deberá seleccionar entre distintas opciones para obtener el supuesto premio. Además, se le insta a compartir la campaña entre sus amistades en WhatsApp.

De esa forma, el atacante expande su ataque abarcando más usuarios para ser afectados. Luego es dirigido a sitios de baja reputación para descargar extensiones, registrarse a sitios de criptomonedas y webs con publicidad, entre otros.

Observación

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

Indicadores de compromiso

Texto Mensaje:
Bono Copec Combustible

URL sitio redirección:
http://anotherbeetle[.]top/cge-cl/tb.php

URL sitio falso:
https://inquirypatch[.]top/snBXDygg/cge-cl

Otros antecedentes

Certificado Digital

Fecha Valido	:	11-04-2022
Fecha Termino	:	10-07-2022
Emitido	:	Let's Encrypt E1

Datos Alojamiento y Dominio

IP	:	[172.67.133.106]
Número de sistema autónomo (AS)	:	13335
Etiqueta del sistema autónomo	:	CLOUDFLARENET
País	:	US
Registrador	:	ARIN
Información del registrador Dominio	:	Alibaba.com Singapore E-Commerce

nsaje


CGE Energía ¡Subsidios energéticos del Gobierno!
3 junio, 2022
¡Felicidades!
CGE Energía ¡Subsidios energéticos del Gobierno!
A través del cuestionario, tendrá la oportunidad de obtener 500000 Peso.
Pregunta 1 de 4: ¿Conoces CGE Energía?
sí
no
Comentario
Amanda Moraes
Genial, nunca he ganado nada, estoy asombrado, ¡gracias a @CGEEnergia por la financiación!
hace 1 minuto
Junior Bianchessi
¡No puedo creerlo! ¡Gané un regalo, gracias @CGEEnergia!
hace 3 minutos
gabriel ferreira
¡Pensé que era una broma, pero fue entregado esta mañana! ¡Muy sorprendido! @CGEEnergia es la mejor empresa que he conocido!
Hace 7 minutos
marcio antonio
¡Gracias @CGEEnergia! De verdad, tengo un regalo. ¡Se lo conté a mis amigos para que ellos también lo consigan!
hace 9 minutos
Denise Ricci
Asistí, muchas gracias! Gané y lo recibí hoy.
hace 10 minutos
Rene Oliveira
Me encantan estas actividades! ¿Existen otras actividades subvencionadas? @CGEEnergia
hace 12 minutos
Maria Hildete Pereira
Pensé que era una broma, pero mi familia y yo recibimos regalos hoy, espero que más personas respondan la encuesta @CGEEnergia
Hace 15 minutos
vicente galvao
¿Hay otras encuestas para realizar?
hace 17 minutos
vanesa mora
¿De Verdad? ¿Cuándo puedo recibirlo?
Hace 20 minutos
Fernando Lopes Galvao
Es cierto, tengo un regalo, ¿lo recibiste?
hace 25 minutos
© 2022 CGE Energía Inc.


Energía ¡Subsidios energéticos del Gobierno!
en este enlace para reclamar el subsidio de
cge-cl/tb.php?jusvmgwy165420673
FALSO
CSIRT


CGE Energía ¡Subsidios energéticos del Gobierno!
3 junio, 2022
¡Felicidades!
CGE Energía ¡Subsidios energéticos del Gobierno!
A través del cuestionario, tendrá la oportunidad de obtener 500000 Peso.
Pregunta 1 de 4: ¿Conoces CGE Energía?
sí
no
FALSO
CSIRT

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: 2022.06.03 11:48:20 -04'00'