Alerta de seguridad informática	8FPH21-00453-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de diciembre de 2021
Última revisión	14 de diciembre de 2021

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.

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 WhatsApp, en la que supuestamente la persona ha sido seleccionada por el Supermercado Líder para participar en una encuentra y recibir una tarjeta de regalo de $400.000

Para esto, el atacante incluye un enlace para dirigir a la víctima a un sitio falso, similar al del supermercado, y ahí contestar la encuesta. Al finalizar el cuestionario, se le solicita a la persona compartir la campaña entre sus amistades.

De esta forma, el atacante obtiene sus credenciales y propaga la estafa a través de sus contactos por WhatsApp.

Observación

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

Indicadores de compromiso

URL sitio falso:

https://studiocustomers[.]com/

Otros antecedentes

Certificado Digital

Fecha Válido	:	17-11-2021
Fecha Término	:	15-02-2022
Emitido	:	Let's Encrypt R3

Datos Alojamiento

IP	:	[172.67.74.50]
Número de sistema autónomo (AS)	:	13335
Etiqueta del sistema autónomo	:	CLOUDFLARENET
País	:	US
Registrador	:	ARIN

Datos del Dominio

Nombre de dominio	:	sourcestring[.]com
Creado	:	22-06-2021
Expira	:	22-06-2026
Información del registrador	:	Google LLC
ID IANA	:	895
Correo electrónico	:	registrar-abuse@google.com
Servidores de nombres	:	johnathan.ns.cloudflare.com lisa.ns.cloudflare.com

Imagen del sitio


Enhorabuena!!
Hoy 14 Diciembre, 2021. Has sido seleccionado al azar para participar en esta encuesta. Sólo te llevará un minuto y podrás recibir un premio: ¡Una tarjeta regalo de 400000$!
Como cada Martes elegimos a 100 usuarios al azar para darles la posibilidad de ganar fabulosos premios. El premio de hoy son 400000$ para poder comprar en cualquier tienda!*.
Sólo 10 afortunados serán los ganadores y sólo si vives en Chile!
Esta encuesta sólo se realiza con fines estadísticos para mejorar el servicio de los usuarios.
Sólo tienes 0 minutos y 00 segundos para poder participar.
Lider
400000$
FALSO
CSIRT
Pregunta 1 de 4:
¿Eres hombre o mujer?
Hombre
Mujer
Más opiniones
50 de 80
Andrés Montoya
Recibí una llamada de que había ganado, ¡estoy super feliz!
Martin García
¡Me encantan las ofertas como esta!
Pablo Silvent
He ganado, he ganado!!! hoy a celebrarlo!!
Amelia Montalbán
Es posible que me envien hoy mi tarjeta de regalo?, gracias
Alejandro Ruiz
¡Eso es genial, nunca había ganado nada!
Andrea Martinez
Al principio pensé que era una broma, pero conseguí mi tarjeta regalo de 400000$, se lo he dicho a mis amigos para que puedan obtener la suya lol
Anabel Silvestre
¿Alguna vez has visto algo por el estilo?, quizás tuviste un mal día, puedes intentarlo más veces!
Rosa Fuentes
¡Participe, gané y en 5 días recibí mi tarjeta, muchas gracias chicos!
Nicolas Pérez
Pensé que era una broma, pero la tarjeta de regalo me llegó esta mañana por correo me gustaría hacer más encuestas!.
Luisa García
Mierda no ganó nada :(
Marcos Quevedo
¿Alguna otra encuesta que pueda hacer?
Lider
400000$
¡LO HAS CONSEGUIDO!
¡Has conseguido la tarjeta de 400000$!
Sigue las siguientes instrucciones y estarás un paso más cerca de tu tarjeta regalo!!
OK
Andrés Montoya
Recibí una llamada de que había ganado, ¡estoy super feliz!
Me gusta · Comentar · 39 · 14 Diciembre, 2021
Martin García
¡Me encantan las ofertas como esta!
PROMOCIÓN COMPRA ONLINE DE 400000$
Introduce los datos para poder entregar el premio
Por favor, introduzca los datos para entregarle el premio.
- Elige -
Introduzca su nombre
Primer y segundo apellido
Seleccione una región
Seleccione una comuna
+56
9
Celular (8 digit...
Todos los campos son obligatorios para validar su participación
Declaro ser mayor de 18 años
Información Básica sobre Protección de Datos [+]

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: 2021.12.14 15:48:15 -03'00'