Alerta de seguridad informática	8FPH21-00449-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	02 de diciembre de 2021
Última revisión	02 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, que indica falsamente a quienes reciben sus mensajes, que el supermercado Jumbo se encuentra de aniversario y, como promoción especial, está regalando una tarjeta de $50.000 pesos.

Con tal de cumplir su objetivo, el atacante incluye un vínculo, supuestamente para que la víctima participe en la promoción. La víctima, al presionar el enlace, es direccionada a un sitio fraudulento semejante al del supermercado, dónde se le invita a completar una encuesta y participar en el sorteo. Al concluir las preguntas, al usuario se le solicita compartir esta campaña entre sus amistades en WhatsApp. De esta forma, el atacante obtiene sus credenciales y la propia víctima propaga la estafa a través de sus contactos de WhatsApp.

Observación

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

Indicadores de compromiso

URL redirección:
http://crowdeddiminish[.]website/jumbo/tb.php?_t=1638457335163845751921 5

URL sitio falso:
https://ekpved[.]tw/nsM1DvIa/jumbo/?_t=1638474116820#1638474123738

URL sitio propaganda:
https://s1.l-o-a-d-i-n-g[.]biz/?p3=7037196158078288247#
https://s.prizeoffer[.]net/win?round=1&tid=5t31p2hzr5qjbfkh8ca8sgwgo,15426683
https://download-step1[.]com/download.html?an=vi&cid=c63b0qde8uobgwj648

Otros antecedentes

Certificado Digital

Fecha Valido	:	20-11-2021
Fecha Término	:	18-02-2022
Emitido	:	Let's Encrypt R3

Datos Alojamiento

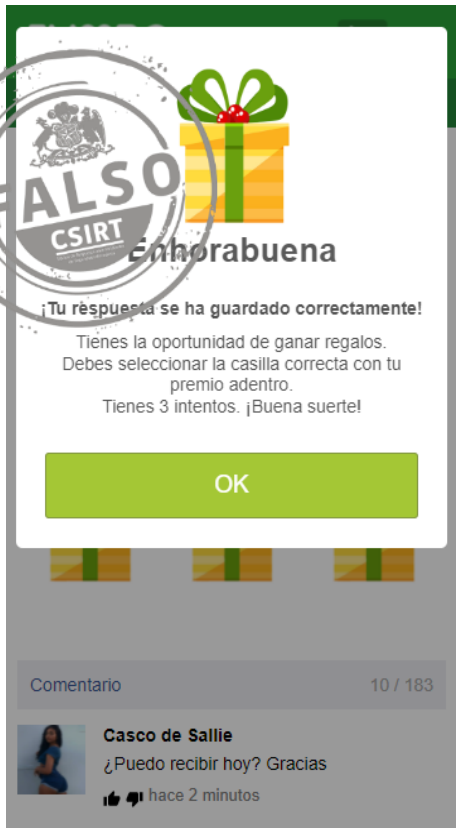
IP	:	[104.21.79.85]
Número de sistema autónomo (AS)	:	13335
Etiqueta del sistema autónomo	:	CLOUDFLARENET
País	:	TR
Registrador	:	RIPE NCC

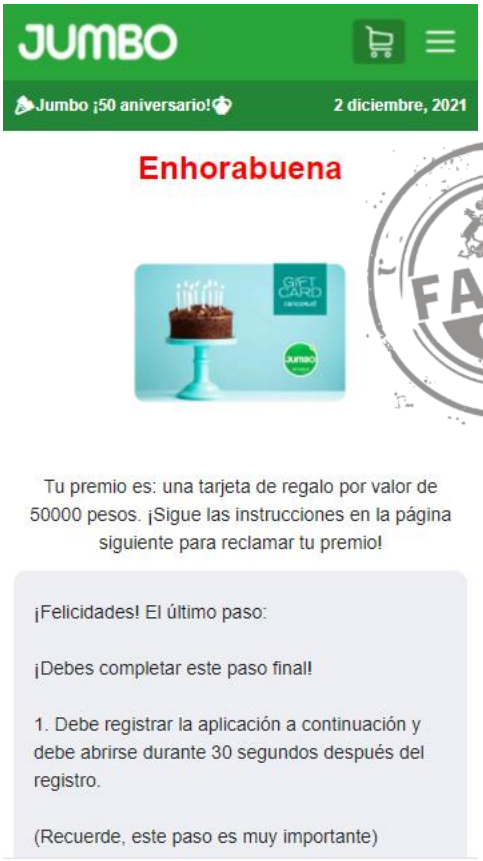
Datos del Dominio

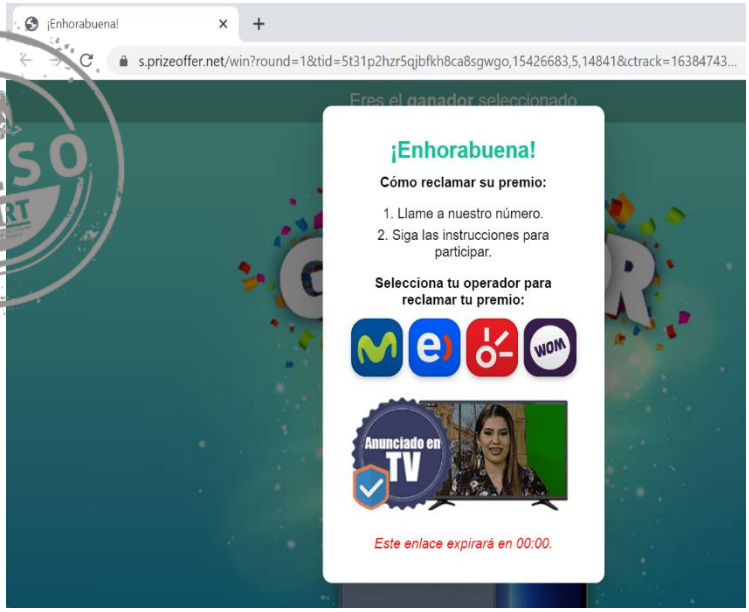
Nombre de dominio	:	ekpved[.]tw
Creado	:	22-04-2021
Expira	:	22-04-2022
Información del registrador	:	no aplica
ID IANA	:	no aplica
Correo electrónico	:	apasabnolittper858@rambler.ru
Servidores de nombres	:	sima.ns.cloudflare.com vicky.ns.cloudflare.com

Imagen del mensaje

Imagen del sitio




JUMBO
Jumbo ¡50 aniversario!
2 diciembre, 2021
Enhorabuena
GIFT CARD
Tu premio es: una tarjeta de regalo por valor de 50000 pesos. ¡Sigue las instrucciones en la página siguiente para reclamar tu premio!
¡Felicidades! El último paso:
¡Debes completar este paso final!
1. Debe registrar la aplicación a continuación y debe abrirse durante 30 segundos después del registro.
(Recuerde, este paso es muy importante)


¡Enhorabuena!
s.prizeoffer.net/win?round=1&tid=5t31p2hzr5qjbfkh8ca8sgwgo,15426683,5,14841&ctrack=16384743...
Eres el ganador seleccionado
¡Enhorabuena!
Cómo reclamar su premio:
1. Llame a nuestro número.
2. Siga las instrucciones para participar.
Selecciona tu operador para reclamar tu premio:
WOM
Anunciado en TV
Este enlace expirará en 00:00.

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: 2021.12.02 17:29:40 -03'00'