Alerta de seguridad cibernética	8FPH20-00150-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	31 de Marzo de 2020
Última revisión	31 de Marzo de 2020

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), ha identificado una campaña de phishing vía WhatsApp, indicando a quienes lo reciben que el supermercado Jumbo se encuentra de aniversario y, como promoción especial, está regalando un cupón de $50.000 pesos para celebrar. El atacante disponibiliza un vínculo para que la víctima participe en la promoción. La víctima, al presionar el enlace, es direccionado a un sitio 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 (20 amigos o 5 grupos), acción necesaria para obtener su cupón. Luego de realizar el paso anterior es direccionado a un sitio semejante al de Jumbo, solicitando las credenciales de acceso. De esta forma el atacante obtiene sus credenciales y además propaga a través de sus contactos de WhatsApp la estafa.

OBSERVACIÓN

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

INDICADORES DE COMPROMISO

Urls sitio falso:

https[:]//myluckyday[.]club/es/jumbo/#

IMAGEN DEL MENSAJE

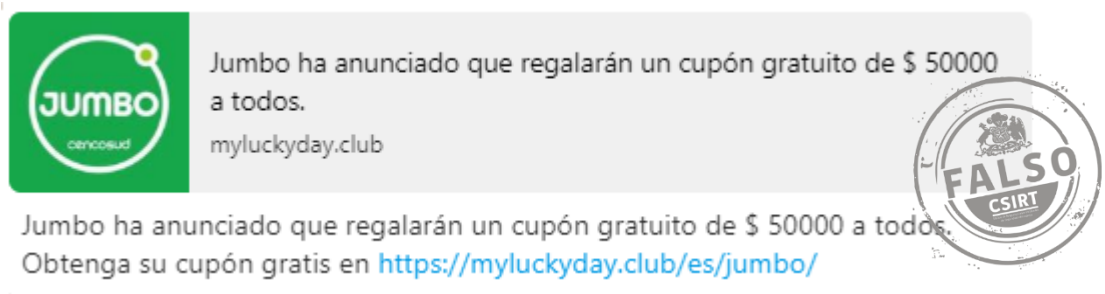
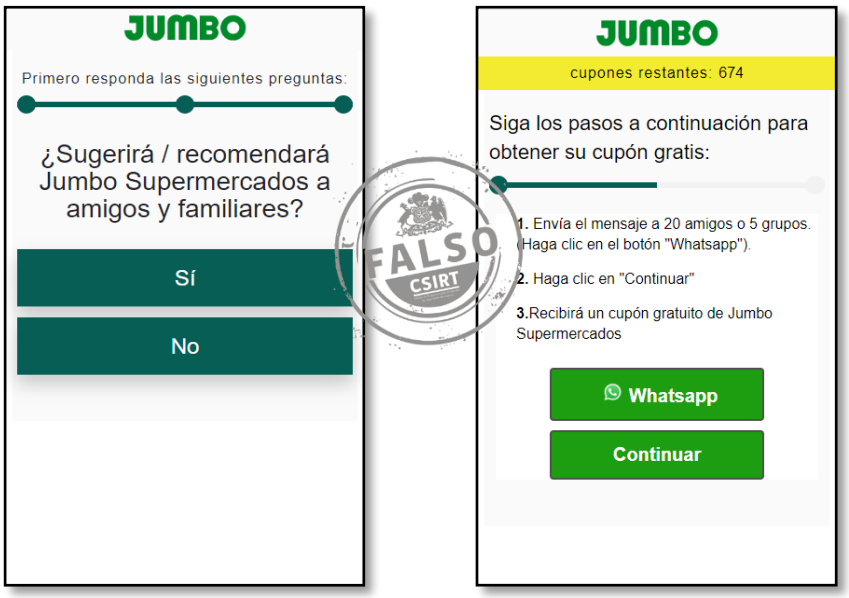


IMAGEN DEL SITIO



RECOMENDACIONES

- No abrir correos ni mensajes de dudosa procedencia.
- Desconfiar de los enlaces y archivos en los mensajes o correo.
- Ser escépticos frente ofertas, promociones o premios increíbles que se ofrecen por internet
- Prestar atención en los detalles de los mensajes o redes sociales
- Mantener sus dispositivos actualizados
- Mantener las aplicaciones actualizadas
- Desconfiar de promociones que no se encuentren en los canales oficiales
  Siempre visitar los canales de comunicaciones oficiales

CSIRT Gobierno de Chile
Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.03.31 23:08:45 -03'00'