

Alerta de seguridad informática	8FPH20-00254-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	24 de Junio de 2020
Última revisión	24 de Junio 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 afectada 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), advierte sobre una campaña de phishing que se está difundiendo a través de WhatsApp supuestamente proveniente del supermercado Líder.

El atacante intenta persuadir a la persona para utilizar un enlace en el mensaje.

El mensaje informa que el supermercado solidariza con el País y regalará cupones de \$100.000 durante la pandemia.

El atacante disponibiliza un enlace en el cual la víctima, al seleccionarlo, es dirigida a una encuesta que debe completar para recibir el supuesto beneficio. Al terminar la encuesta aparece un supuesto proceso de verificación, donde se le solicita compartir el mensaje de la promoción con, al menos, 20 contactos de WhatsApp. De esta manera el atacante expande su ataque abarcando la mayor cantidad de usuarios posibles. Luego, la víctima es dirigida a otro sitio donde se le solicita información como el correo electrónico y contraseña. Luego es direccionada nuevamente a otro sitio pidiendo los datos de su tarjeta de crédito.

Observación

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

Indicadores de compromiso

Urls sitio falso:

hxxp://cupon-lider[.]com
hxxps://junebox[.]me/markets/es/lider/

Urls Redirecciones:

Body SHA-256 sitio falso

4b4618fa5848765aa557346ed4a9acc7bf9cee3ad08ae3cd22128244f133bd6d

Certificado Digital

Fecha Valido :
Fecha Termino :
Emitido :

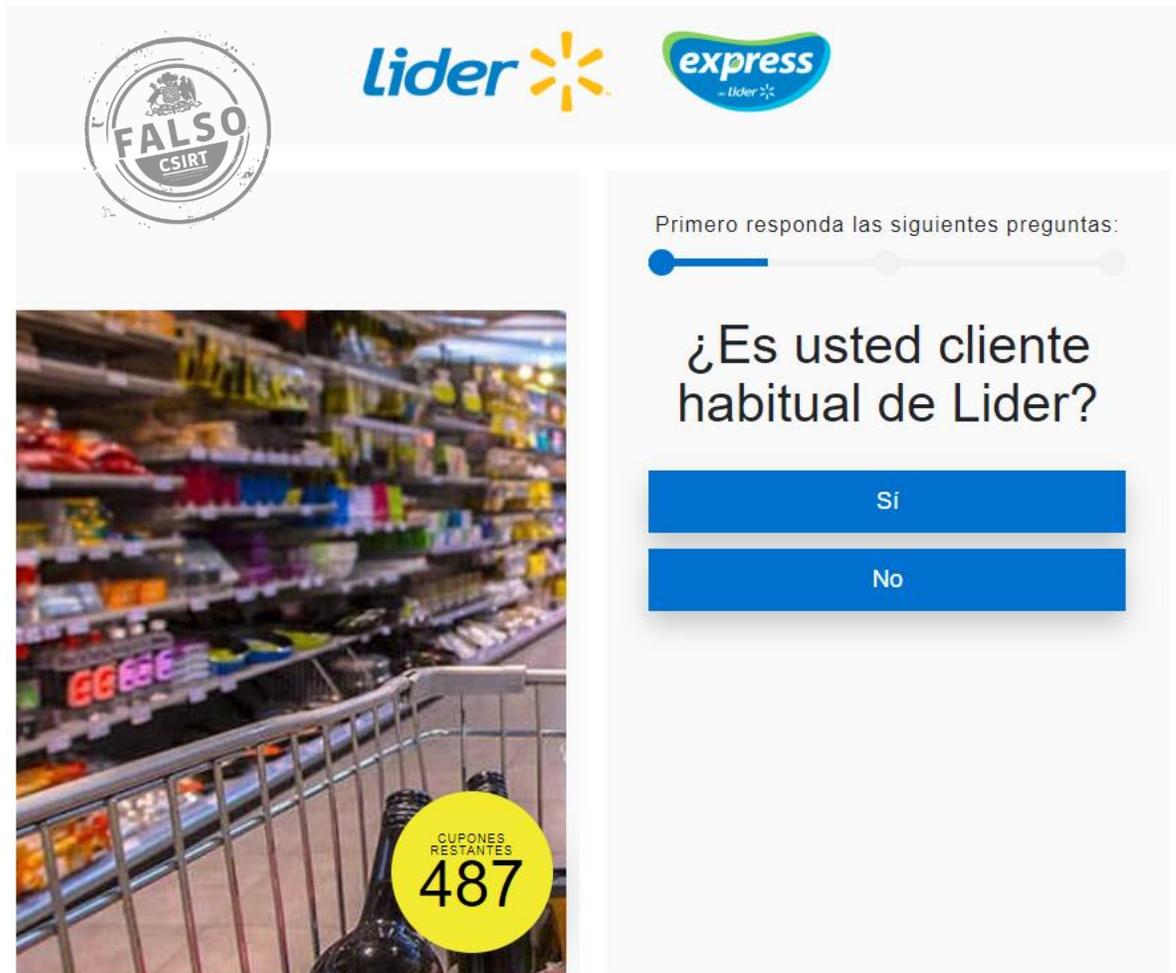
Datos Alojamiento

IP : 45.148.120.2
Número de sistema autónomo (AS) : 64425
Etiqueta del sistema autónomo : SKB Enterprise B.V.
País : Países Bajos
Registrador : RIPE

Datos del Dominio

Nombre de dominio : cupon-lider[.]com
Estado del dominio : clientTransferProhibited addPeriod
Creado : 19-06-2020
Expira : 19-06-2021
Información del registrador : NameSilo, LLC
ID IANA : 1479
Correo electrónico : abuse@namesilo.com
Servidores de nombres : ns15.flaunt7.com, ns16.flaunt7.com

Imagen del sitio



The screenshot shows a survey interface for LIDER. At the top left, there is a circular stamp that says "FALSO CSIRT". The header features the "Lider" logo and the "express" logo. The main content area contains the text "Primero responda las siguientes preguntas:" followed by a progress bar. The question is "¿Es usted cliente habitual de Lider?". Below the question are two blue buttons labeled "Si" and "No". On the left side of the survey, there is a photograph of a shopping cart in a supermarket aisle. A yellow circular sticker on the cart reads "CUPONES RESTANTES 487".



Consigue una tarjeta de regalo de \$100.000

Quedan 18 minutos y 8 segundos
Aprovecha esta oferta.

RELLENA LA INFORMACIÓN A CONTINUACIÓN

Correo Electrónico

Contraseña

CONTINUE

Participa en el sorteo para tener la oportunidad de ganar una tarjeta regalo de \$100.000. El afortunado ganador será contactado por correo electrónico.

junebox - Thakshila Goonewardena LTD 400 Deans Road, 10, Colombo, Sri Lanka
Contact: info@junebox.live

¿Por qué necesitamos su información de facturación??

Al unirse a este servicio, disfrutará de una prueba de 5 días en el programa de nuestro socio. Si continúa con una suscripción más allá del período de prueba de 5 días, se le cobrará un monto en su tarjeta de crédito que varía, dependiendo de la elección de decinueve a noventa euros. Cuando la contribución será deducida de su tarjeta de crédito u otro método de pago, mantendrá acceso a estos servicios, que están reservados exclusivamente a los miembros que pagan por el acceso en el sitio web de nuestro socio.

¿Cómo puedo obtener mi regalo de bienvenida?

En junebox.live, todos los miembros deben tener 18 o más años para suscribirse. Esto significa que las personas menores de 18 años no pueden tener acceso a nuestras promociones. Ninguna persona con menos de 18 años podrá suscribirse en ni pagar con tarjeta de crédito por nuestros servicios.

¿Existe limitación de edad?

En junebox.live, todos los miembros deben tener 18 o más años para suscribirse. Esto significa que las personas menores de 18 años no pueden tener acceso a nuestras promociones. Ninguna persona con menos de 18 años podrá suscribirse en ni pagar con tarjeta de crédito por nuestros servicios.

¿Hay algún pago adicional que no se haya discutido?

Nos aseguramos de proporcionarles a nuestros miembros un historial de transacciones detallado para que sepan lo que están pagando. La información de la tarjeta de crédito es necesaria únicamente para facilitar futuras compras. No aparecerá ningún cobro en el estado de cuenta de su tarjeta de crédito, a menos que actualice a una membresía premium o que realice una compra. Si crea una cuenta, acepta automáticamente nuestros términos y condiciones.



Séguro y protegido



¿Por qué necesitamos sus datos de facturación?

Como somos los únicos con licencia para distribuir nuestro contenido a ciertos países, le pedimos que verifique su dirección de correo proporcionándonos un número de tarjeta de crédito válido. GARANTIZAMOS que NO se aplicarán cargos por la verificación de su cuenta. Ningún cargo aparecerá en el estado de cuenta de su tarjeta de crédito, a menos que usted se registre a una Suscripción Premium o haga una compra.

Inscríbese hoy mismo. Le decimos por qué:

- ✓ ¡Haga clic y vea! - ¡sin esperar!
- ✓ Descargue películas, ¡en un instante!
- ✓ ¡Transmita películas en vivo con calidad HD!
- ✓ ¡Garantizada para ahorrarle tiempo!
- ✓ ¡Funciona en su TV, PC o MAC!

Nunca habrá cargos ocultos

Nos aseguramos de suministrar a nuestros miembros un historial detallado de sus transacciones para que sepan lo que están pagando. La información de sus tarjetas de crédito se necesita únicamente para facilitar futuras compras. Ningún cargo aparecerá en el estado de cuenta de su tarjeta de crédito, a menos que usted se registre a una Suscripción Premium o haga una compra. Al crear una cuenta, usted está de acuerdo con nuestros [Términos y condiciones](#).

¿Preguntas? ¿Comentarios?

Démos una llamada al **1-92-529-6112**

¡Al completar esta transacción, usted certifica que está de acuerdo con los [Términos y Condiciones](#) que ha leído nuestro [Política de privacidad](#). Esta oferta incluye 7 días de prueba gratis de musicstream. Luego de 7 días, la suscripción a musicstream se renueva automáticamente por \$49.95 por mes. Si desea cancelar, SOLO CANCELE SU MEMEBREIA ANTES DEL PERIODO DE PRUEBA PARA EVITAR CARGOS.

Verificación de cuenta

Una suscripción \$0.00

Nombre

Apellido

Área postal/Código postal

País

Número de tarjeta

Fecha de vencimiento

CVW

¿Dónde está mi CVW?

VERIFICAR SU CUENTA >

Todos los usuarios están protegidos por bonumedia.com Guarantee. Su información está segura y protegida porque protegemos la información de nuestros miembros mediante el uso de las mejores medidas de seguridad posibles. bonumedia.com no venderá ni alquilará su información privada a terceros, porque valoramos su privacidad.

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.
- Vislizar los sitios web que se ingresen sean los oficiales.