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 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), 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	:	

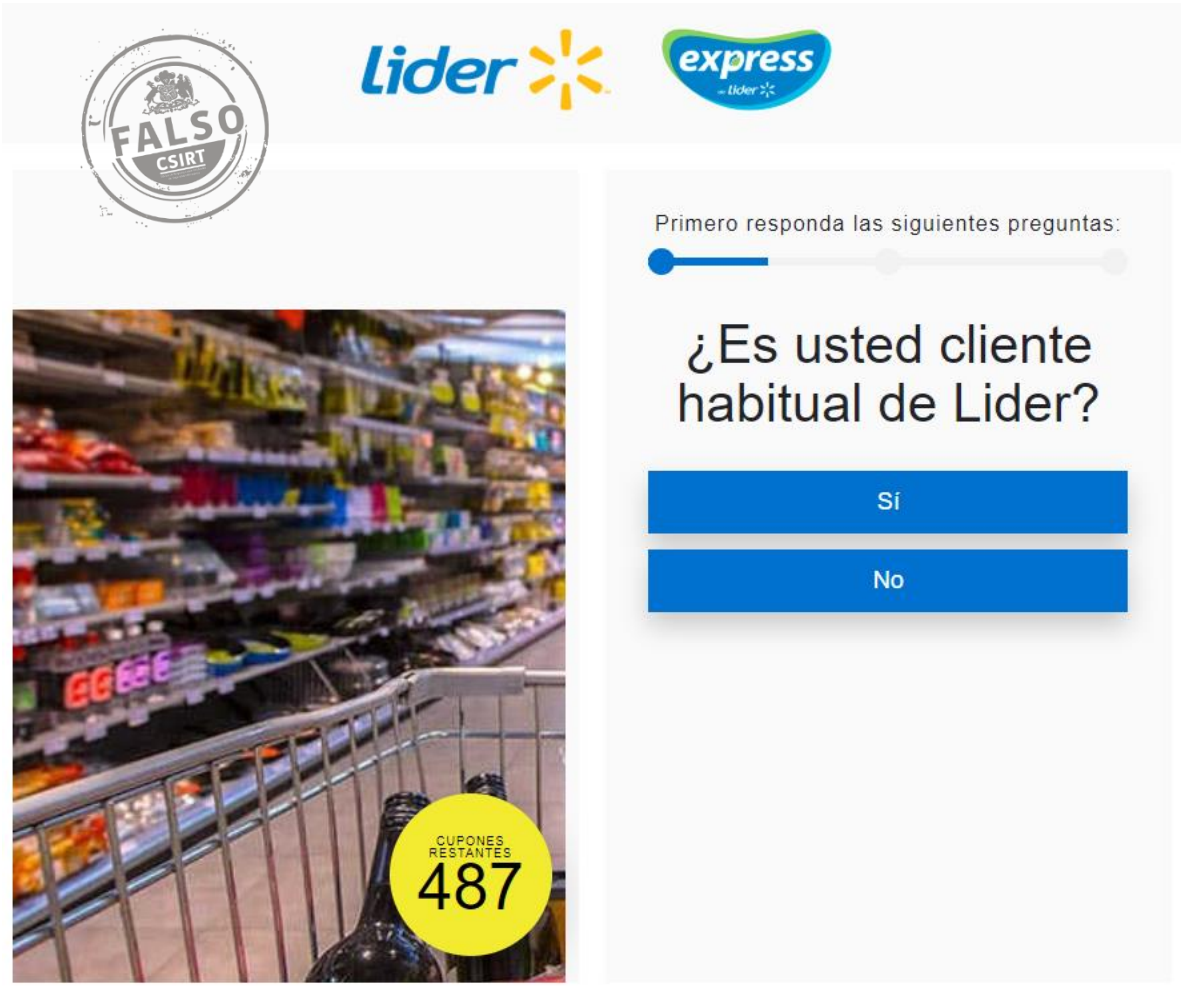
Datos Alojamiento

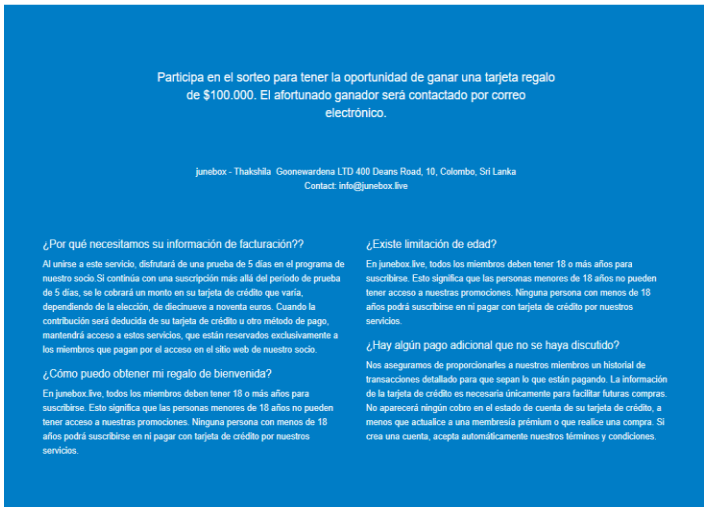
IP	:	45.148.120.2
Número de sistema autónomo (AS)	:	64425
Etiqueta del sistema autónomo	:	SKB Enterprise B.V.
País	:	Países Bajos
Registrador	:	RIPE

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





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.