

Alerta de seguridad cibernética	8FFR21-01026-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	30 de noviembre de 2021
Última revisión	30 de noviembre 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 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 fraude 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 fraude, 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 del Gobierno de Chile (CSIRT de Gobierno) ha identificado la activación de una página fraudulenta que suplanta a la tienda Rosen, y podría servir para robar credenciales bancarias.

Lo anterior constituye una falsificación de la marca institucional que podría afectar a usuarios, clientes y a la entidad aludida.

Indicadores de compromiso

URL sitio falso

[https://www.camasshopcl\[.\]shop/](https://www.camasshopcl[.]shop/)

Certificado Digital

Fecha Válido	25-10-2021
Fecha Término	23-01-2022
Emitido	Let's Encrypt R3

Datos Alojamiento

IP	[5.255.62.142]
Número de Sistema Autónomo (AS)	197328
Etiqueta del Sistema Autónomo	Istanbuldc Veri Merkezi Ltd Sti
País	TR
Registrador	RIPE NCC

Datos del Dominio

Nombre de Dominio	camasshopcl[.]shop
Creado	25-10-2021
Expira	25-10-2022
Información del Registrador	NAMECHEAP INC
ID IANA	1068
Correo Electrónico	abuse@namecheap.com
Servidores DNS	dns1.registrar-servers.com dns2.registrar-servers.com

Imagen del sitio





Carrito de compras



Realizar pedido

DIRECCIÓN DE ENVÍO

* Indica Campos Requeridos

* Nombre

Nombre
Ingrese nombre válido

* Apellido

Apellido
Ingrese apellido valido

* Dirección De Envío

Nombre y número de edificio y calle, nombre de la empresa, etc.
Ingrese Dirección 1 válida

Dirección De Envío (Continuación)

Número de apartamento/habitación, piso, edificio, etc.

* Ciudad

Ciudad
Ingrese ciudad válida

* Estado/ Provincia

Valparaiso

* Código Postal

Código postal
Ingrese correo postal válido

* País/ Región

Chile

* Número De Movil

Número de movil
Ingrese teléfono válido

Número De Movil 2

Número de movil 2

* Correo Electrónico

Pago

RESUMEN DE PAGO

Subtotal	\$12.264
Primeros pedidos ahorran (10%)	-\$1.226
(+) Cargos de Envío y Seguro	+\$12.264

Gran total **\$23.302**

REALIZAR PEDIDO

MÉTODOS DE PAGO DISPONIBLES



 Carrito de compras —  Realizar pedido —  Pago

Número de pedido
0301211130233224278

Dirección de envío

Carrito Total	\$12.264
Primeros pedidos ahorran(-10%)	-\$1.226
(+) Cargos de Envío y Seguro	+\$12.264
Gran total	\$23.302

FORMAS DE PAGO

TARJETA DE CRÉDITO

   

Número de Tarjeta

Fecha de vencimiento

CVN [¿Qué es esto?](#)

 **PAGAR AHORA (\$23.302)**



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.