

Alerta de seguridad cibernética	8FFR21-00904-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	25 de Febrero de 2021
Última revisión	25 de Febrero 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 loC 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 loC 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 (CSIRT), ha identificado la activación de una página fraudulenta en un dominio chileno que intenta suplantar a la empresa DHL, la que podría servir para robar credenciales de usuarios.

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.cursosadity\[.\]cl/demo/Shipmentsonline/MARKET/MARKET/](https://www.cursosadity[.]cl/demo/Shipmentsonline/MARKET/MARKET/)

Certificado Digital

Fecha Válido	14-02-2021
Fecha Término	15-05-2021
Emitido	Let's Encrypt R3

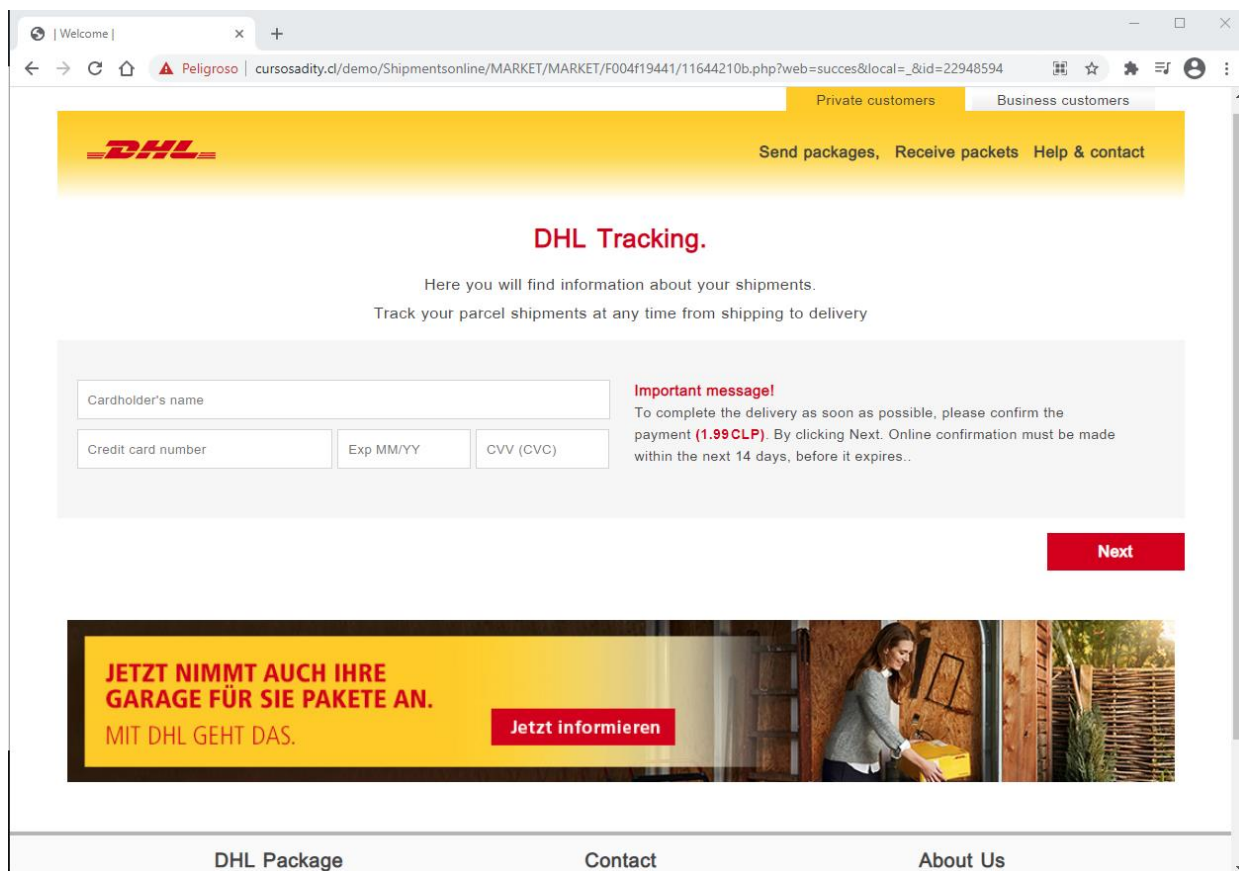
Datos Alojamiento

IP	[209.124.90.240]
Número de Sistema Autónomo (AS)	55293
Etiqueta del Sistema Autónomo	A2HOSTING
País	US
Registrador	ARIN

Datos del Dominio

Nombre de Dominio	cursosadity[.]cl
Creado	18-11-2016
Expira	18-11-2022
Información del Registrador	Nic Chile
ID IANA	
Correo Electrónico	abuse@nic.cl
Name Server	ns20912490240.a2dns.com ns2091249024.a2dns.com

Imagen del sitio



The screenshot shows a web browser window displaying the DHL Tracking page. The browser's address bar shows the URL: `corsosadity.cl/demo/Shipmentsonline/MARKET/MARKET/F004f19441/11644210b.php?web=succes&local=_&id=22948594`. The page features a yellow header with the DHL logo and navigation links for "Private customers" and "Business customers". Below the header, there are links for "Send packages", "Receive packets", and "Help & contact". The main heading is "DHL Tracking.", followed by a sub-heading: "Here you will find information about your shipments. Track your parcel shipments at any time from shipping to delivery". A form section contains input fields for "Cardholder's name", "Credit card number", "Exp MM/YY", and "CVV (CVC)". To the right of the form is an "Important message!" section with the text: "To complete the delivery as soon as possible, please confirm the payment (1.99 CLP). By clicking Next. Online confirmation must be made within the next 14 days, before it expires..". A red "Next" button is positioned below the form. At the bottom of the page, there is a banner with the text: "JETZT NIMMT AUCH IHRE GARAGE FÜR SIE PAKETE AN. MIT DHL GEHT DAS." and a red button labeled "Jetzt informieren". The footer contains links for "DHL Package", "Contact", and "About Us".

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.