Alerta de seguridad cibernética	8FFR21-00987-01
Clase de alerta	Fraude
Tipo de incidente	Falsificación de Registros o Identidad
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Julio de 2021
Última revisión	07 de Julio 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 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 pagina fraudulenta que suplanta al servicio de entrega de encomiendas DHL, la que podría servir para robar las credenciales de sus 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://mail.cabconnect.com[.]au/images/wet/2020dhl_topscript/dhl_topscript/cmd-login=cd01efe09a3c34091edcbd69433f3bbc/?reff=MDg1ODI4MGI1NTA4ZWUxMDk1OGE3NWVkNTExOGE3Nzg=

Certificado Digital

Fecha Válido	15-05-2021
Fecha Término	13-08-2021
Emitido	R3

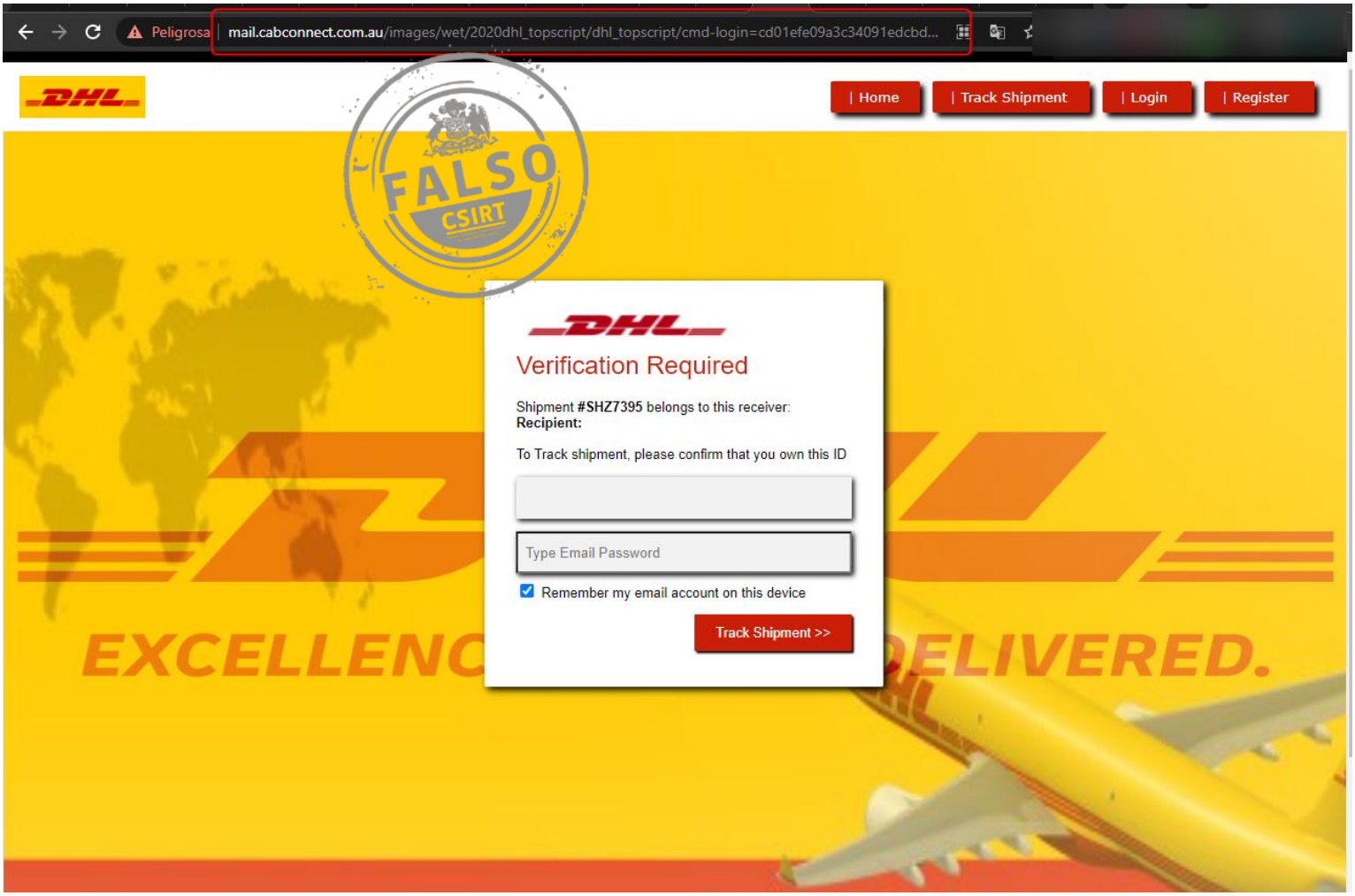
Datos Alojamiento

IP	[162.222.226.104]
Número de Sistema Autónomo (AS)	394695
Etiqueta del Sistema Autónomo	PUBLIC-DOMAIN-REGISTRY
País	US
Registrador	ARIN

Datos del Dominio

Nombre de Dominio	cabconnect.com[.]au
Creado	NO APLICA
Expira	NO APLICA
Información del Registrador	serverRenewProhibited
ID IANA	NO APLICA
Correo Electrónico	NO APLICA
Name Server	ns1.cp-26.webhostbox.net ns2.cp-26.webhostbox.net

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

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2021.07.07 12:29:49 -04'00'