Alerta de seguridad informática	2CMV22-0307-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	19 de julio de 2022
Última revisión	19 de julio de 2022

NOTIFICACIÓN

La información consignada en el presente informe es producto del análisis de múltiples fuentes, de terceras partes e investigación propia del CSIRT de Gobierno. 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.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT) de Gobierno ha identificado una nueva campaña de phishing con malware que se hace pasar como proveniente de DHL Express.

En esta campaña, los delincuentes indican falsamente a la víctima que "*Su paquete ha llegado a la oficina. nuestro servicio de mensajería no pudo entregarlo en su dirección debido a una dirección incorrecta proporcionada por nuestro cliente. Para recibir su paquete, diríjase a cualquiera de nuestras oficinas más cercanas y muestre este recibo. Haga clic en el archivo adjunto para descargar e imprimir el recibo*." Al descargar el archivo y ser ejecutado se gatilla la infección del equipo.

Familia de malware: Troyano

Observación

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

IoC Archivo

Archivos que se encuentran en la amenaza

Nombre: DHL_119040 de recibo,pdf.img
SHA256: a3ba3f9f24cb4588b5f5943e1f06b96ca25d425424e804c30074e624c164d14e

Nombre: DHL_119040 de recibo,pdf.exe
Nombre: HGHJJKYUHJJJDSD456.exe
SHA256: 6576ca8629f0a914f2689637d670f0b1fc58b3bd0d9d3a04d3a32e716496dee8

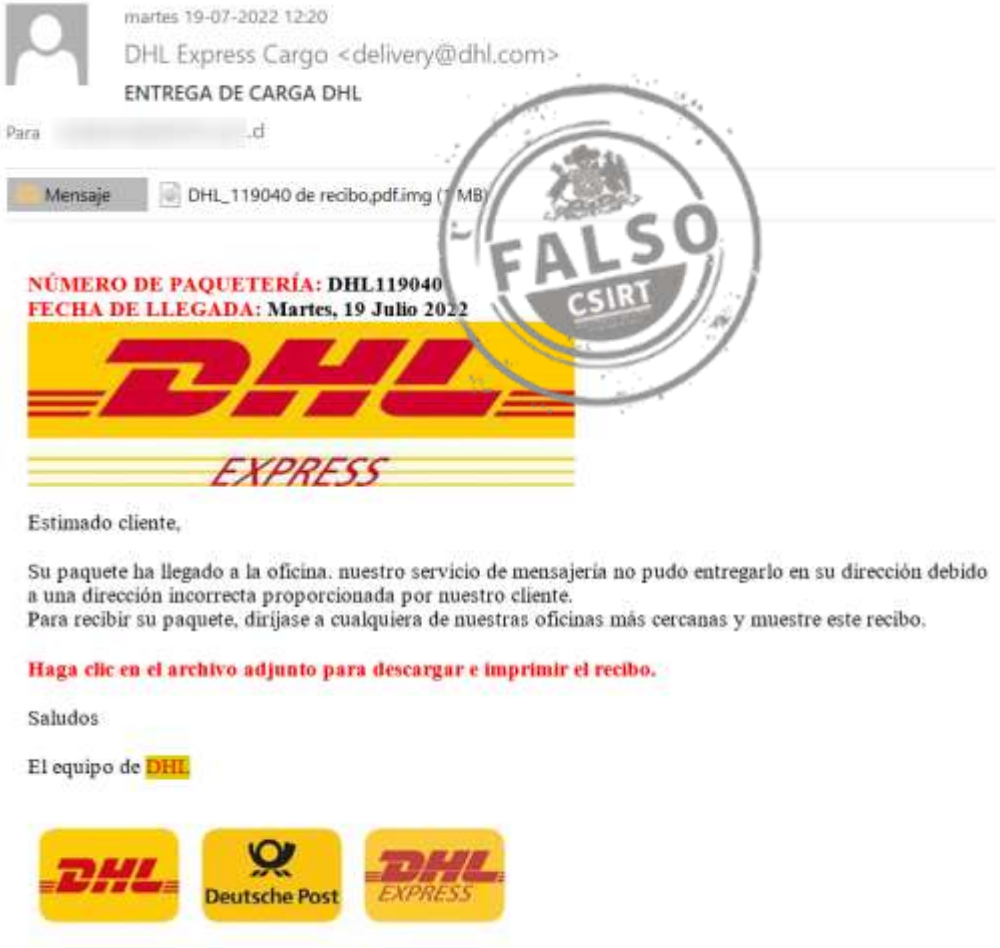
Dominios / URL / IP:

mail.tycautomotriz[.]cl

https://secure.comodo[.]com/CPS0L
http://ocsp.sectigo[.]com/
http://ocsp.comodoca[.]com/
http://ocsp.usertrust[.]com/

[131.72.236.163]

Imagen del Mensaje



martes 19-07-2022 12:20

DHL Express Cargo <delivery@dhl.com>

ENTREGA DE CARGA DHL

Para [redacted].cl

Mensaje DHL_119040 de recibo.pdf.img (1 MB)

NÚMERO DE PAQUETERÍA: DHL119040
FECHA DE LLEGADA: Martes, 19 Julio 2022

DHL EXPRESS

Estimado cliente,

Su paquete ha llegado a la oficina. nuestro servicio de mensajería no pudo entregarlo en su dirección debido a una dirección incorrecta proporcionada por nuestro cliente.
Para recibir su paquete, diríjase a cualquiera de nuestras oficinas más cercanas y muestre este recibo.

Haga clic en el archivo adjunto para descargar e imprimir el recibo.

Saludos

El equipo de DHL

DHL Deutsche Post DHL EXPRESS

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.