Alerta de seguridad informática	2CMV21-0230-01
Clase de alerta	Fraude
Tipo de incidente	Malware
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	12 de octubre de 2021
Última revisión	12 de octubre 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.

Resumen

El Equipo de Respuesta ante Incidentes de Seguridad Informática (CSIRT de Gobierno) ha identificado una campaña de malware. El atacante busca persuadir a las personas de descargar un archivo adjunto y que este sea ejecutado en su equipo, donde gatillará la infección del malware.

Para convencer a su víctima, el mensaje del correo suplanta a DHL e indica falsamente que se adjunta una supuesta guía aérea en referencia al próximo arribo de su producto, siendo realmente malware.

Observación

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

IoC Correo Electrónico

Datos del encabezado del correo

Correo electrónico
@coldimport.com.pe

Servidor de Correo
hwsrv-909060.hostwindsdns.com [23.254.202.75]

Asunto
DHL Agencia de Aduanas - Notificación antes del arribo de su envío con guía aérea

IoC Archivo

Archivos que se encuentran en la amenaza

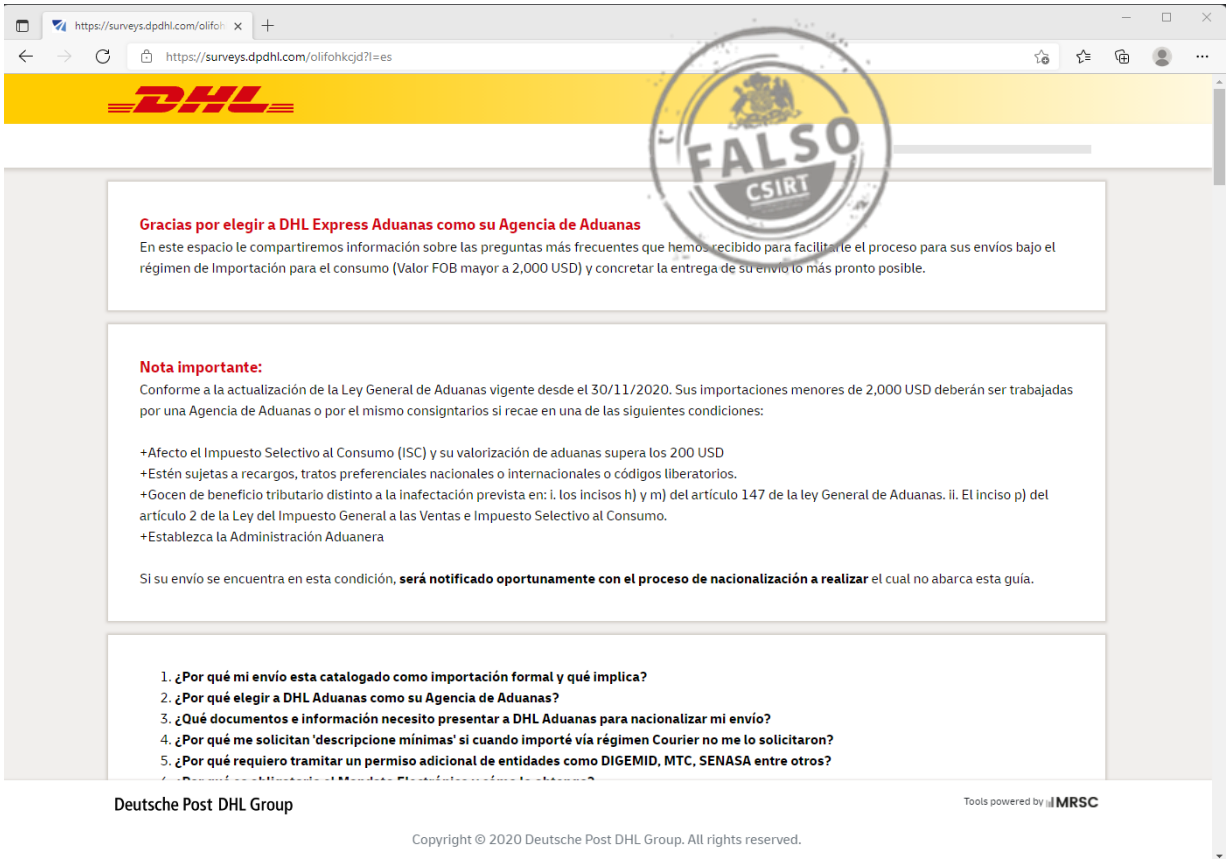
Nombre : 2961221_211004171515866.img
SHA256 : 2C61B110A73C1500A26B65B187BC3DFAD7367921213B95AAFC19887D132EF2D4

Nombre : 2961221_211004171515866.exe
SHA256 : DB125EA0B4C9F1EA9A2634240EA3A4CDF3A317FA545BC98E83367802CFB1B3D8

IoC Archivo

https://dpdhl.sharefile[.]eu/d-sa75ff29482164e1

Imagen del Mensaje



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: 2021.10.12 11:00:53 -03'00'