Alerta de Seguridad Informática (2CMV-00021-001)

Nivel de Riesgo: Alto

Tipo: Phishing - Malware

Fecha de lanzamiento original: 17 de Julio de 2019 | Última revisión 17 de Julio de 2019

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 del Gobierno de Chile (CSIRT), ha identificado una campaña de Phishing con Malware, indicando que existe una encomienda sellada que contiene un documento. Este correo intenta engañar a quienes lo reciben al señalar que proviene de la empresa DHL.

El atacante incita a las víctimas a descargar un documento que, supuestamente, es la declaración completa de la encomienda. El documento es un archivo ISO, el que al ser ejecutado desencadena la infección.

Indicadores de compromisos

Smtp Host

Server[.]nelsonleonardo[.]com [66.7.216.128]

From: (Falso)

dhlemalship@dhl.com

Subject:

Aviso de llegada envió de DHL

Archivo

Nombre : documento de recibo de dhl
MD5 : c1f95f5577fe6cfe689055f013989171
SHA256 : 1dd23399117bace024125378e42771fcc18d12a2b93f3d76a4c23d0d74e30138

Imagen

DHL EXPRESS <dhlemalship@dhl.com> undisclosed-recipients:

Aviso de llegada envío de DHL - Número de emisión 6091843704

AVISO DE LLEGADA

Estimado Cliente,

Notificación de envío

Un paquete sellado que contiene documentos ha sido enviado para ser entregado a usted.
Fecha de envío: **15-07-2019, 08:39:29**
Servicio: DHL aire
Descripción: Factura de prioridad
cuenta Remitente final: *****047293
Cust. Ref: N/A

Para la declaración completa información en cuanto al paquete expedido, por favor descargue el archivo adjunto.amablemente mantener segura la información descargada, necesitaremos que les proporcionan para confirmar cuando nuestro agente te ofrece tu parcela a usted.
Nos gustaría darle las gracias por aceptar los servicios de DHL Express.

Saludos cordiales,

Este correo electrónico es escaneado(garantizado) y enviado a usted porque usted está suscrito a nuestro boletín de noticias.
Nota: Si el mensaje se encuentra POR ERROR EN SU junk mail amablemente abierto como iguales.

© 2019 DHL Express | Servicio Al Cliente | www.dhl.com

Recomendaciones

- Mantener actualizadas sus plataformas (Office, Windows, Adobe Acrobat, Oracle Java y otras)
- 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

Contactos

https://www.csirt.gob.cl
+ (562) 24863850
@CSIRTGOB
https://www.linkedin.com/company/csirt-gob

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2019.07.17 18:20:08 -04'00'