

Alerta de seguridad informática	8FPH21-00387-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Abril de 2021
Última revisión	07 de Abril 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 phishing 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 phishing, 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), advierte sobre una campaña de phishing siendo difundida a través de un correo electrónico que supuestamente proviene desde los servicio de seguimiento de DHL.

El atacante busca persuadir a las personas para que abran un enlace adjunto en el cuerpo del correo. El mensaje del correo llama al usuario a completar la entrega de un paquete confirmando un pago solicitado. Al seleccionar el enlace para ver más detalles, las personas son dirigidas a un sitio falso, donde se exponen al robo de sus credenciales.

Observación

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

Indicadores de compromiso

Urls sitio redirección:

[https://taniaeyanga\[.\]com/Shipment/Tracking/](https://taniaeyanga[.]com/Shipment/Tracking/)

Urls sitio falso:

[https://taniaeyanga\[.\]com/Shipment/Tracking/F004f19441/11644210b.php?web=succes&local=_&id=70405351](https://taniaeyanga[.]com/Shipment/Tracking/F004f19441/11644210b.php?web=succes&local=_&id=70405351)

Asunto:

Tracking Number 525488547124

Smtip Sender:

jennig3@admin.jenniferkem.com

Smtip Host

[209.59.182.103]

Otros antecedentes

Certificado digital

Fecha Valido : 08-03-2021
Fecha Término : 07-06-2021
Emitido : ZeroSSL RSA Domain Secure Site CA

Datos alojamiento

IP : [160.153.131.205]
Número de sistema autónomo (AS) : 21501
Etiqueta del sistema autónomo : RIPE NCC
País : NL
Registrador : ARIN

Datos del dominio

Nombre de dominio : taniaeyanga[.]com
Creado : 08-02-2019
Expira : 08-02-2022
Información del registrador : GoDaddy.com, LLC
ID IANA : 146
Correo electrónico : abuse@godaddy.com
Servidores de nombres : ns67.domaincontrol.com
ns68.domaincontrol.com

Imagen del mensaje



Tracking Number 525488547124

Este mensaje ha sido identificado como un correo no deseado. Se eliminará después de 10 días. [No es un correo no deseado](#)



DHL Delivery <tracking@dhl.com>

Mar 06-04-2021 15:07

Para: Usted



ATT00001

288 bytes

Your package is ready for delivery.

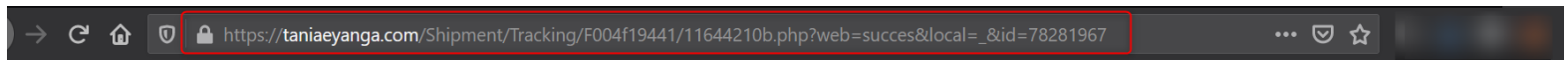
1. **In order to complete the delivery of your package [525488547124](#), please confirm the payment (1.99). Online confirmation must be made within the next 48 hours, before it expires**

[Deliver My Package Now >>](#)


Kind regards,
DHL Tracking services.

[Responder](#) | [Reenviar](#)

Imagen del sitio




Private customers Business customers



Send packages, Receive packets Help & contact

DHL Tracking.

Here you will find information about your shipments.
Track your parcel shipments at any time from shipping to delivery



Credit card number Exp MM/YY CVV (CVC)

Important message!
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..

Next

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.