Alerta de seguridad informática	8FPH20-00110-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	07 de Febrero de 2020
Última revisión	07 de Febrero de 2020

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), ha identificado una campaña de phishing a través de un correo electrónico supuestamente proveniente de DHL.

El mensaje en inglés informa a la víctima que su paquete fue devuelto a la oficina de DHL por el no pago del costo de envío. El atacante intenta persuadir al usuario para que seleccione el enlace que se encuentra en el cuerpo del correo, indicando que tiene un plazo de 72 horas para realizar el pago. Al seleccionar el vínculo, la víctima es dirigida a un sitio semejante al de DHL donde se expone al robo de sus datos personales y a los de su tarjeta de crédito.

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

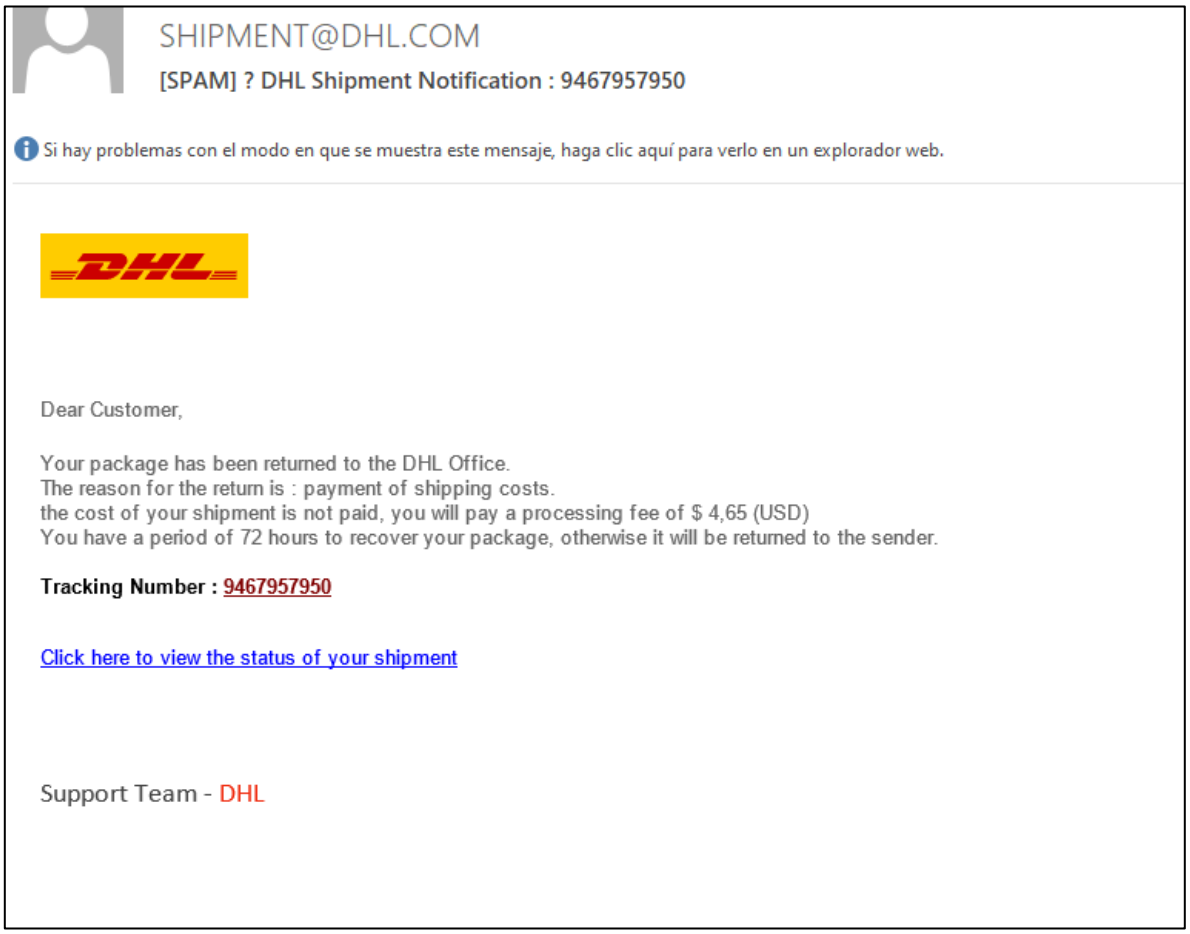
Indicadores de compromisos
Urls
http[:]//bit[.]do/frZe2
http[:]//sacepalmero[.]com/6EZ95KP9EV33601DZZ/63E655PPUMORLSIKER/03SA5EZR98RPLOR/
http[:]//vivadhlexpress[.]com/0ZE6F5ZD9OZPLR/trackshipment-dhl36001/FR869EITERTKKDALDA/TARCDDK-SUIVE36501/ZZA6S12565110DDEDZ/TRACK30600/01dhl-information-contact[.]html
http[:]//sacepalmero[.]com/ZE65ERD5APEMROEI/0VFS1J6RYPMALSOA/6DEZ5AF01RPDZMFOEZ/TARCDDK-SUIVE36501/DEA69D5110DDEDZ/TRACK30600/01dhl-payment-billing[.]html
http[:]//sacepalmero[.]com/ZE65ERD5APEMROEI/0VFS1J6RYPMALSOA/6DEZ5AF01RPDZMFOEZ/TARCDDK-SUIVE36501/DEA69D5110DDEDZ/TRACK30600/01dhl-payment-completed[.]html

Sender
SHIPMENT[@]dhl[.]com

Smtp Host
[193.26.21.149]
[193.26.21.88]
[193.26.21.113]

Subject
DHL Shipment Notification : 9467957950

Imagen del correo



SHIPMENT@DHL.COM

[SPAM] ? DHL Shipment Notification : 9467957950

Si hay problemas con el modo en que se muestra este mensaje, haga clic aquí para verlo en un explorador web.

Dear Customer,

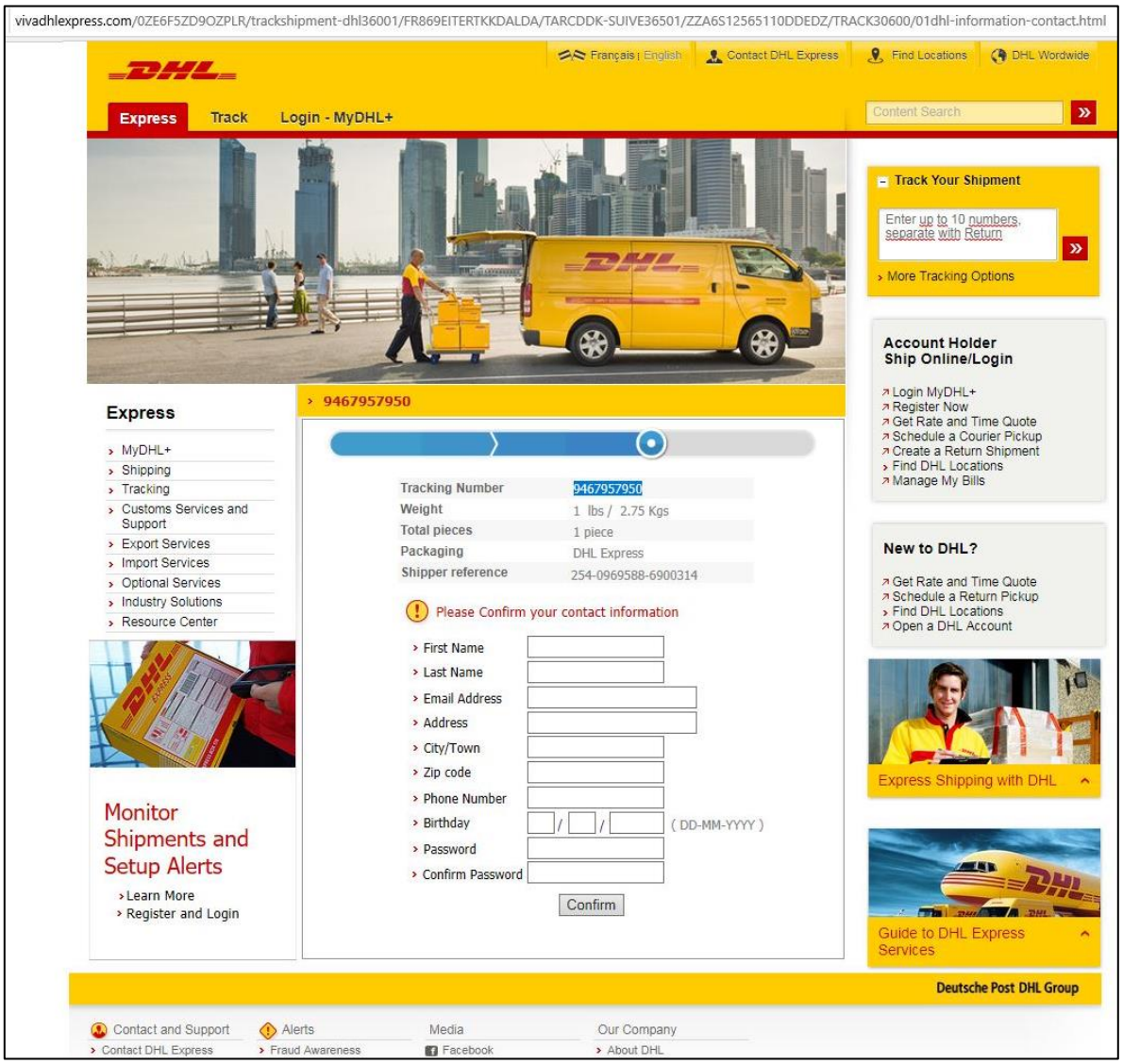
Your package has been returned to the DHL Office.
The reason for the return is : payment of shipping costs.
the cost of your shipment is not paid, you will pay a processing fee of $ 4,65 (USD)
You have a period of 72 hours to recover your package, otherwise it will be returned to the sender.

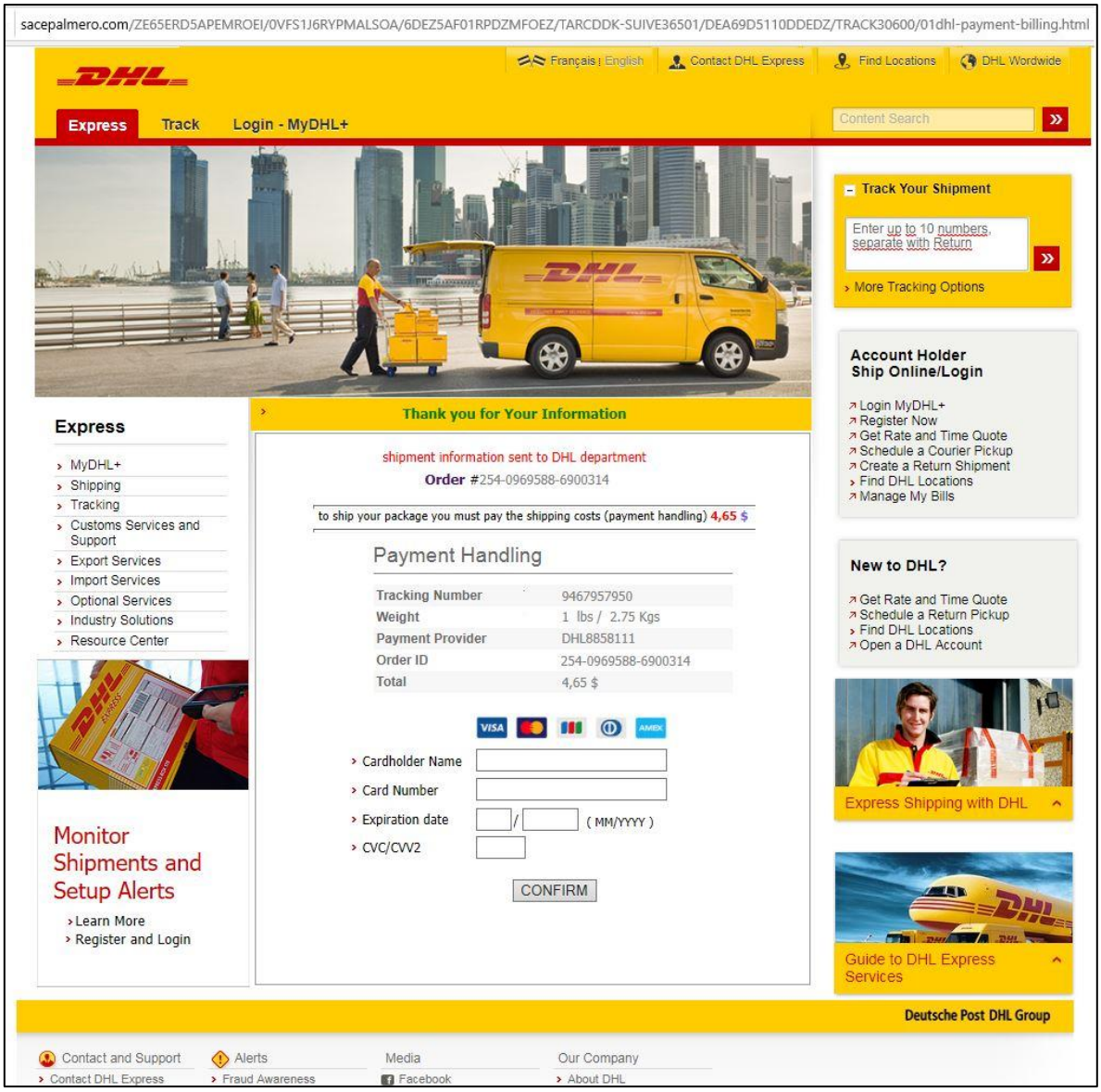
Tracking Number : 9467957950

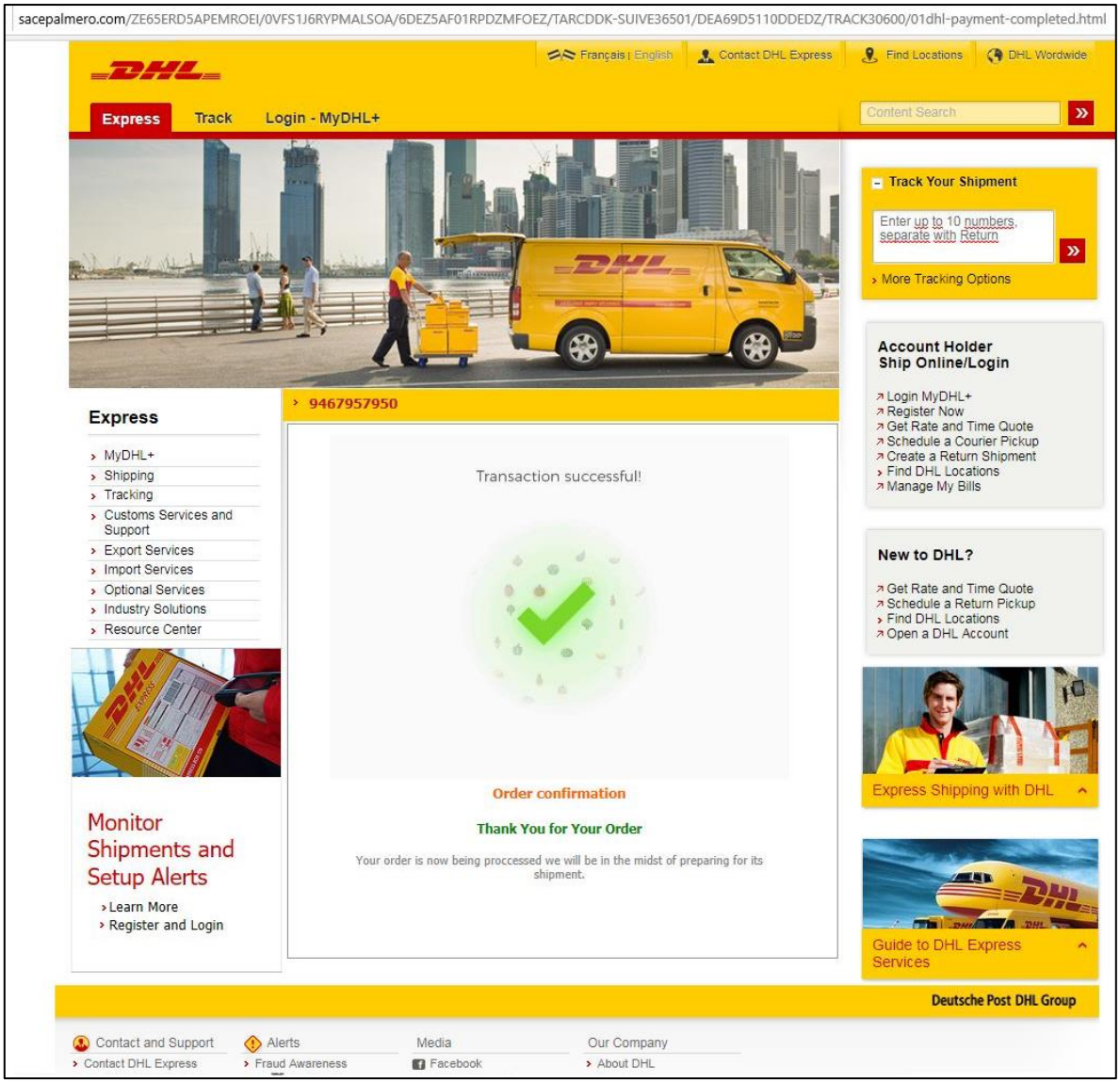
Click here to view the status of your shipment

Support Team - DHL

Imagen Sitio Web




sacepalmero.com/ZE65ERD5APEMROEI/0VFS1J6RYPMALSOA/6DEZ5AF01RPDZMFOEZ/TARCDDK-SUIVE36501/DEA69D5110DDEDZ/TRACK30600/01dhl-payment-billing.html
Français | English
Contact DHL Express
Find Locations
DHL Wordwide
Express
Track
Login - MyDHL+
Content Search
Track Your Shipment
Enter up to 10 numbers, separate with Return
More Tracking Options
Account Holder
Ship Online/Login
Login MyDHL+
Register Now
Get Rate and Time Quote
Schedule a Courier Pickup
Create a Return Shipment
Find DHL Locations
Manage My Bills
Thank you for Your Information
shipment information sent to DHL department
Order #254-0969588-6900314
to ship your package you must pay the shipping costs (payment handling) 4,65 $
Payment Handling
Tracking Number 9467957950
Weight 1 lbs / 2.75 Kgs
Payment Provider DHL8858111
Order ID 254-0969588-6900314
Total 4,65 $
Cardholder Name
Card Number
Expiration date
(MM/YYYY)
CVC/CVV2
CONFIRM
Express
MyDHL+
Shipping
Tracking
Customs Services and Support
Export Services
Import Services
Optional Services
Industry Solutions
Resource Center
Monitor Shipments and Setup Alerts
Learn More
Register and Login
New to DHL?
Get Rate and Time Quote
Schedule a Return Pickup
Find DHL Locations
Open a DHL Account
Express Shipping with DHL
Guide to DHL Express Services
Deutsche Post DHL Group
Contact and Support
Contact DHL Express
Alerts
Fraud Awareness
Media
Facebook
Our Company
About DHL



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

CSIRT Gobierno de Chile

Firmado digitalmente por CSIRT Gobierno de Chile
Fecha: 2020.02.07 15:29:02 -03'00'