Alerta de seguridad cibernética	8FPH20-00267-01
Clase de alerta	Fraude
Tipo de incidente	Phishing
Nivel de riesgo	Alto
TLP	Blanco
Fecha de lanzamiento original	14 de Julio de 2020
Última revisión	14 de Julio 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), advierte sobre una campaña de phishing que se está difundiendo a través de un correo electrónico que supuestamente proviene del servicio de envíos DHL.

El atacante busca persuadir a las personas para el uso de un enlace en el cuerpo del correo.

El mensaje, en idioma inglés, advierte a quien lo recibe sobre el eventual arribo de una encomienda para el día de hoy, pero solicita confirmar la dirección.

Al seleccionar el enlace para confirmar la dirección, la persona es dirigida a un sitio falso de DHL, donde se expone al robo de sus credenciales.

Observación

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

INDICADORES DE COMPROMISO

Urls sitio falso:
hxxps://storage[.]googleapisvcom/dhl-parcel-tracking[.]appspot[.]com/trackingdeliveryorderesupdateshere/DHL[.]html

Sender
humptex2000[@]gmail[.]com

Smtp Host
[124.110.96.72]

Asunto
DHL PARCEL ARRIVAL NOTICE

Otros antecedentes

URL Body SHA-256

1276f0255c07c798b505e039eff1470322eed51ae1d445207eabd9a1b16b6620

Certificado Digital

Fecha Valido	:	17-06-2020
Fecha Termino	:	09-09-2020
Emitido	:	Google Trust Services

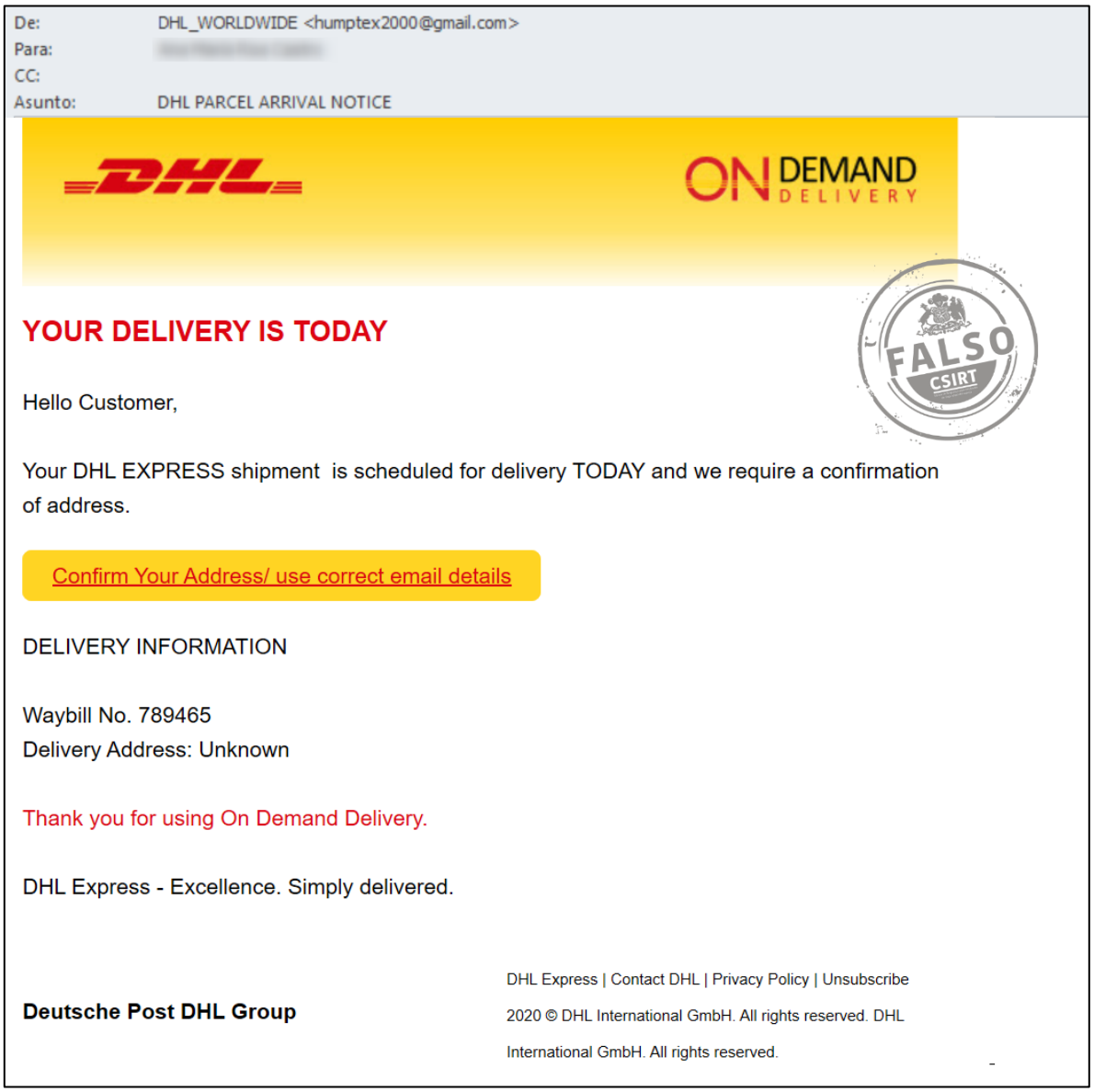
Datos Alojamiento

IP	:	172.217.212.128
Número de sistema autónomo (AS)	:	AS 15169
Etiqueta del sistema autónomo	:	Google LLC
País	:	Estados Unidos
Registrador	:	ARIN

Datos del Dominio

Nombre de dominio	:	GOOGLEAPISL.]COM
Estado del dominio	:	clientDeleteProhibited clientTransferProhibited clientUpdateProhibited serverDeleteProhibited serverTransferProhibited serverUpdateProhibited
Creado	:	25-01-2005
Expira	:	25-01-2021
Información del registrador	:	MarkMonitor Inc.
ID IANA	:	292
Correo electrónico	:	abusecomplaints@markmonitor.com
Servidores de nombres	:	NS1.GOOGLE.COM NS2.GOOGLE.COM NS3.GOOGLE.COM NS4.GOOGLE.COM

Imagen del mensaje



De: DHL_WORLDWIDE <humptex2000@gmail.com>
Para:
CC:
Asunto: DHL PARCEL ARRIVAL NOTICE

DHL

ON DEMAND DELIVERY

FALSO CSIRT

YOUR DELIVERY IS TODAY

Hello Customer,

Your DHL EXPRESS shipment is scheduled for delivery TODAY and we require a confirmation of address.

Confirm Your Address/ use correct email details

DELIVERY INFORMATION

Waybill No. 789465
Delivery Address: Unknown

Thank you for using On Demand Delivery.

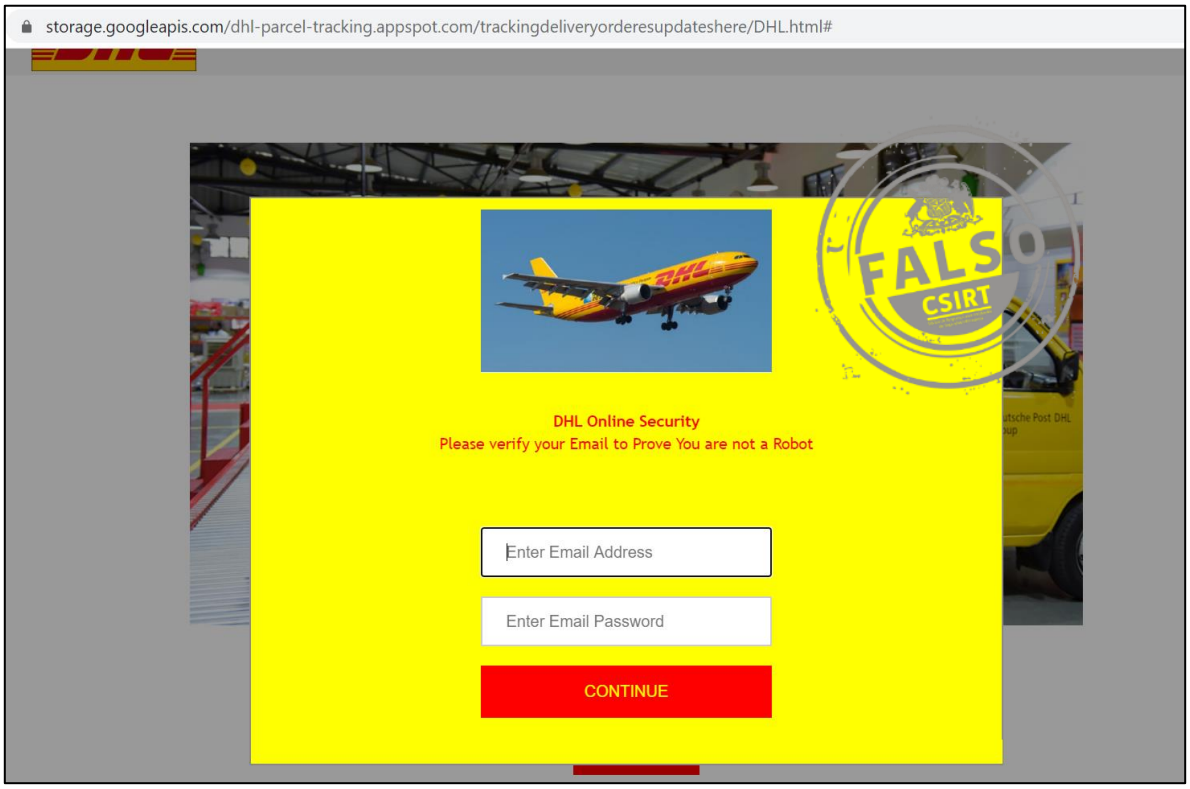
DHL Express - Excellence. Simply delivered.

Deutsche Post DHL Group

DHL Express | Contact DHL | Privacy Policy | Unsubscribe

2020 © DHL International GmbH. All rights reserved. DHL International GmbH. All rights reserved.

Imagen del sitio



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.