20210410, Nota Informativa, INCIBE y OSI.

En virtud de mis compromisos contractuales, seguidamente os actualizo la información de contacto del **INCIBE** (Instituto Nacional de Ciberseguridad) y os traslado las dos últimas alertas del **OSI** (Oficina de Seguridad del Internauta).

Los datos actualizados para poder ponerse en contacto con el INCIBE son los siguientes:

Ciudadanos: incidencias@incibe-cert.es

Empresas: incidencias@incibe-cert.es

Instituciones afiliadas a la red académica y de investigación española (RedIRIS): iris@incibe@cert.es

Operadores esenciales y de infraestructuras críticas: pic@incibe-cert.es

Proveedores de servicios digitales: incidencias@incibe-cert.es

Os recuerdo que la línea de ayuda de ciberseguridad del INCIBE es el número **017**.

Por otra parte, las dos úlimas alertas publicitadas en la página de la OSI (https://www.osi.es/es/actualidad/avisos) considero que son de bastante interés y debemos estar especialmente vigilantes ante ellas; a saber:

1. Correo suplantando a la Agencia Tributaria que busca descargar malware en tu equipo

Se ha detectado una nueva campaña de *phishing* a través de correos electrónicos suplantando a la Agencia Tributaria. El mensaje informa al usuario de una supuesta acción fiscal registrada en su base datos y

para consultarla facilita dos enlaces de acceso a la Sede Electrónica que descargan un archivo *malware*.

Recursos afectados

Cualquier usuario que haya recibido el correo electrónico, haya pulsado sobre alguno de los enlaces y una vez descargado el archivo .zip, lo haya abierto e instalado.

Solución

Si has descargado y ejecutado el archivo malicioso, es posible que tu dispositivo se haya infectado. Para proteger tu equipo, debes escanearlo con un antivirus actualizado o seguir los pasos que encontrarás en desinfección de dispositivos. Si necesitas soporte o asistencia para la eliminación del *malware*, INCIBE te ofrece su servicio de respuesta y soporte ante incidentes de seguridad.

Si no has ejecutado el archivo descargado, posiblemente tu dispositivo no se habrá infectado. Lo único que debes hacer es eliminar el archivo que encontrarás en la carpeta de descargas. También deberás enviar a la papelera el correo de tu bandeja de entrada.

En caso de duda sobre la legitimidad del correo, no pulses sobre ningún enlace y ponte en contacto con la empresa o el servicio que supuestamente te ha enviado el correo, siempre a través de sus canales oficiales de atención al cliente.

Recuerda que, para mayor seguridad, es recomendable realizar copias de seguridad de manera periódica con toda la información que consideres importante para que, en caso de que tu equipo se vea afectado por algún incidente de seguridad, no la

pierdas. También es recomendable mantener tus dispositivos actualizados y protegidos siempre con un antivirus.

Detalles

Se ha detectado una campaña de correos electrónicos suplantando a la Agencia Tributaria cuyo objetivo es engañar al usuario para pulsar sobre cualquiera de los enlaces. Supuestamente los enlaces conducen a una sede electrónica de la Agencia Tributaria donde el usuario puede consultar los detalles de una acción fiscal registrada en una base de datos. La campaña de correos electrónicos identificada, circula bajo el asunto '**Acción fiscal**' y '**Factura no Pagada - Gobierno de España**', aunque no se descarta que existan otros correos con asuntos similares.

El mensaje del correo se caracteriza por:

- Contener imágenes de logotipos oficiales que intentan dar más credibilidad al correo.
- Facilitar un enlace que simula pertenecer la sede electrónica de la Agencia Tributaria, pero que al pulsar sobre él, redirige a un domino que descarga el malware.
- No contener grandes errores ortográficos como es habitual en estos casos.
- Usar un dominio en el correo electrónico del remitente (la parte que va después del @) con palabras relacionadas con el objetivo del fraude, como "agencia-tributaria26" que no pertenece al dominio oficial de la Agencia Tributaria. Debemos recordar que el correo electrónico es bastante sencillo de falsificar.

- Conseguir llamar nuestra atención al aproximarse el periodo para presentar la declaración de la Renta del año fiscal 2020.
- Utilizar mismos formatos de correos con mensajes y asuntos distintos.

Ejemplo 1:

De Agencia Tributaria 370035 <sede-electronica36940@agencia-tributaria26.jdhhuf.es>

Asunto **Acción fiscal**

A

GOBIERNO DE ESPAÑA MINISTERIO DE HACIENDA

Agencia Tributaria

Este correo electrónico se refiere a una acción fiscal registrada en nuestra base de datos.

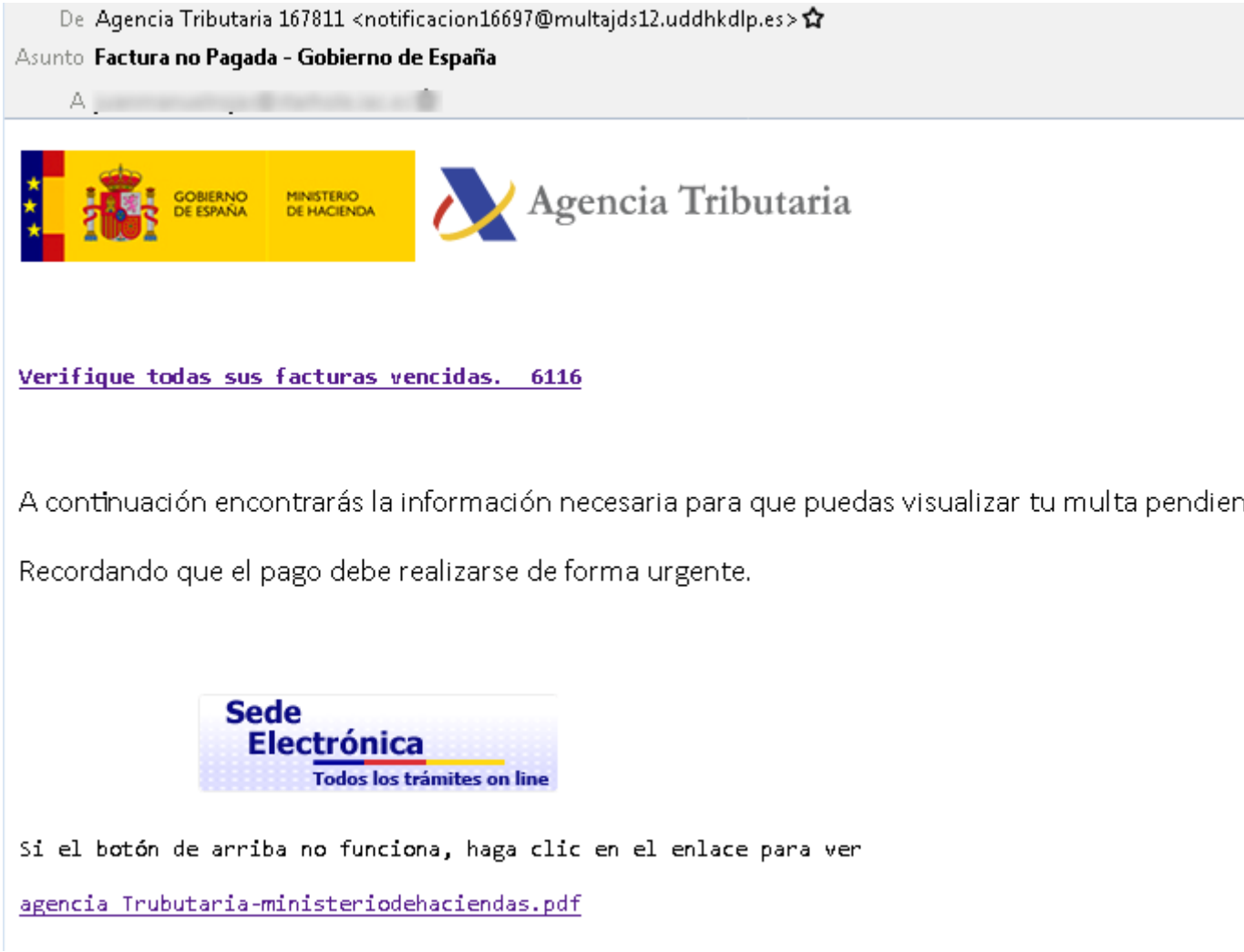
acceder a toda la información en el adjunto a continuación...

Sede Electrónica
Todos los trámites on line

Si no es redirigido por la oficina electrónica, haga clic aquí:
sedeelectonica-action gobiernoespanagob.esjdf.pdf 1875

Actualización 07/04/2021

Ejemplo 2:



Si se pulsa sobre los enlaces, se descargará automáticamente desde el navegador web en el dispositivo un archivo .zip que contiene el malware y que al ejecutarse infectará el dispositivo.

2. Suplantan a la DGT para instalar virus en tu dispositivo

Se ha detectado una campaña fraudulenta a través del correo electrónico (phishing) suplantando a la Dirección General de Tráfico (DGT). El mensaje contiene un enlace a una supuesta notificación que descarga malware en el dispositivo.

Recursos afectados

Cualquier usuario que haya recibido un correo electrónico de estas características, haya pulsado sobre el enlace para consultar el supuesto archivo, y posteriormente haya abierto el fichero que se descarga.

Solución

Si has descargado y ejecutado el archivo malicioso, es posible que tu dispositivo se haya infectado. Para proteger tu equipo, debes escanearlo con un antivirus actualizado o seguir los pasos que encontrarás en desinfección de dispositivos. Si necesitas soporte o asistencia para la eliminación del *malware*, INCIBE te ofrece su servicio de respuesta y soporte ante incidentes de seguridad.

Si no has ejecutado el archivo descargado, posiblemente tu dispositivo no se habrá infectado. Lo único que debes hacer es eliminar el archivo que encontrarás en la carpeta de descargas. También deberás enviar a la papelera el correo de tu bandeja de entrada.

En caso de duda sobre la legitimidad del correo, no pulses sobre ningún enlace y ponte en contacto con la empresa o el servicio que supuestamente te ha enviado el correo, siempre a través de sus canales oficiales de atención al cliente.

Recuerda que, para mayor seguridad, es recomendable realizar copias de seguridad de manera periódica con toda la información que consideres importante para que, en caso de que tu equipo se vea afectado por algún incidente de seguridad, no la pierdas. También es recomendable mantener tus dispositivos actualizados y protegidos siempre con un antivirus.

Detalles

Se ha detectado una campaña de correos electrónicos suplantando a la Dirección General de Tráfico (DGT) que contiene un enlace que, al pulsar sobre él, descarga *malware* (un fichero malicioso) en el dispositivo.

Los correos identificados contienen el siguiente asunto para provocar el interés del usuario '**Bloqueo del Vehiculo – Multa no pagada**', aunque no se descarta que existan otros correos con asuntos diferentes, pero con el mismo objetivo: incitar al usuario a descargar un fichero bajo algún pretexto de su interés, utilizando para ello técnicas de ingeniería social.

Los correos identificados contienen el siguiente asunto para provocar el interés del usuario 'Bloqueo del Vehiculo – Multa no pagada', aunque no se descarta que existan otros correos con asuntos diferentes, pero con el mismo objetivo: incitar al usuario a descargar un fichero bajo algún pretexto de su interés, utilizando para ello técnicas de ingeniería social.

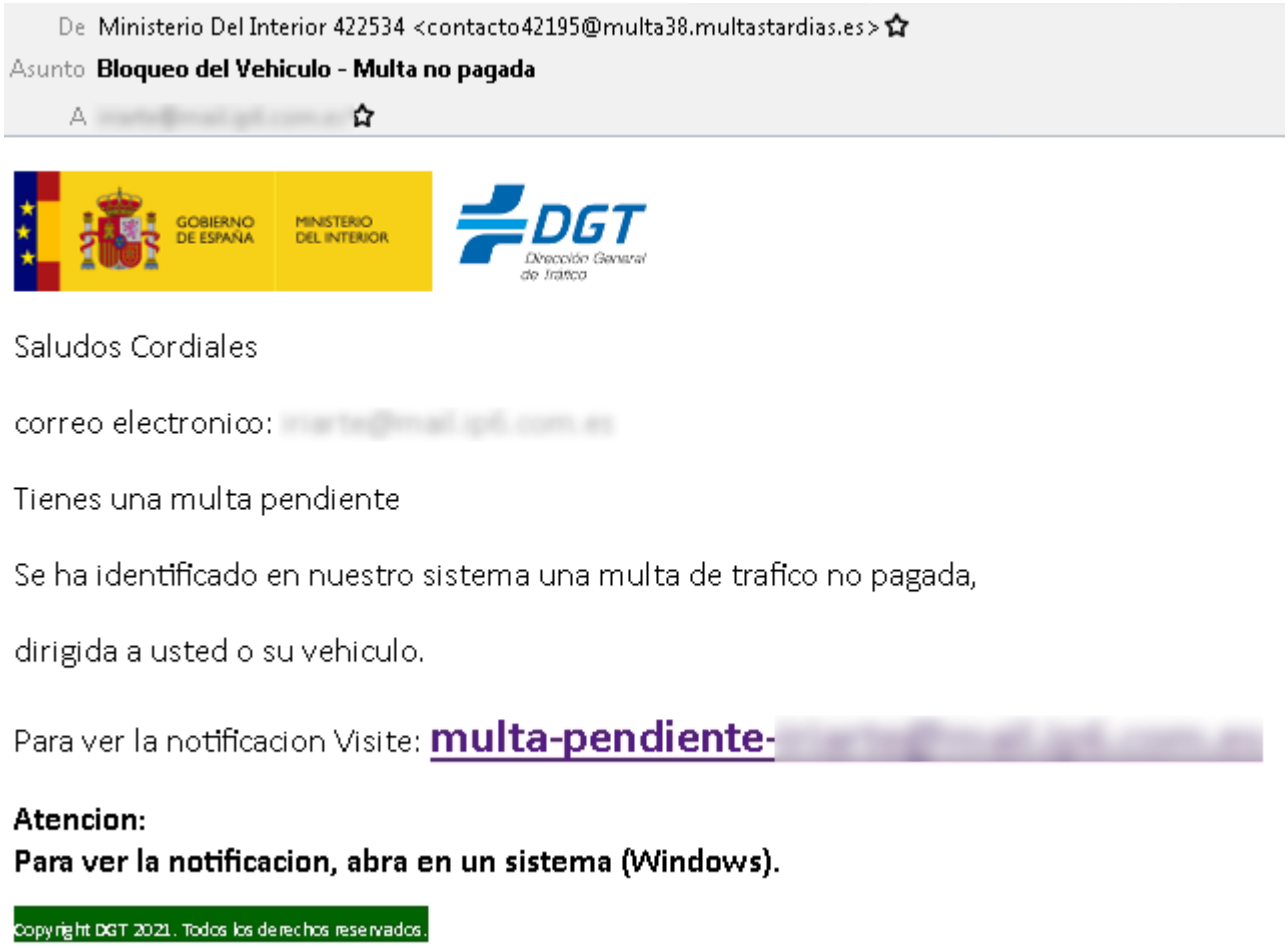
El mensaje del correo se caracteriza por:

- Contener imágenes de logotipos oficiales que intentan dar más credibilidad al correo.
- Facilitar un enlace que simula pertenecer la sede electrónica de la DGT, pero que al pulsar sobre él, redirige a un domino que descarga el malware.
- Incluir textos con faltas de ortografía y mala redacción, lo que facilita su identificación como fraudulento.
- Usar un dominio en el correo electrónico del remitente (la parte que va después del @) con palabras relacionadas con el

objetivo del fraude, como “multanopagada20” y “multasdelministerio”, que no pertenecen al dominio oficial de la DGT. Debemos recordar que el correo electrónico es bastante sencillo de falsificar.

Ejemplo 1:

Ejemplo 2:



De Ministerio Del Interior 422534 <contacto42195@multa38.multastardias.es>

Asunto **Bloqueo del Vehiculo - Multa no pagada**

A

GOBIERNO DE ESPAÑA MINISTERIO DEL INTERIOR

DGT Dirección General de Tráfico

Saludos Cordiales

correo electronico:

Tienes una multa pendiente

Se ha identificado en nuestro sistema una multa de trafico no pagada,

dirigida a usted o su vehiculo.

Para ver la notificacion Visite: **multa-pendiente-**

Atencion:
Para ver la notificacion, abra en un sistema (Windows).

Copyright DGT 2021. Todos los derechos reservados.

En todo caso, y como siempre, quedo a vuestra disposición para aclarar cualquier duda sobre la cuestión comentada.

Hecho conforme a mi leal saber y entender, en Manilva a 10 de abril de 2021,

DELEGADO DE PROTECCIÓN DE DATOS 2019 12 18 ESQUEMA CERTIFICACIÓN AEPD

ZOTANO SANCHEZ SALVADOR - 32028277H

Firmado digitalmente por ZOTANO SANCHEZ SALVADOR - 32028277H
Fecha: 2021.04.10 17:22:55 +02'00'

Salvador Zotano Sánchez

(Delegado de Protección de Datos Certificado 19-ADK0101 conforme al Esquema AEPD-DPD)