OFICINA Acelera pyme

FEMEVAL

PREVISIONES DE LA CIBERSEGURIDAD, CONCIENCIACIÓN DE LOS RIESGOS Y SOLUCIONES PARA LA PYME

20 DE FEBRERO DEL 2024

ESET Digital Security
Progress. Protected.

Financiado por la Unión Europea

red.es

Fondos Europeos

Fondo Europeo de Desarrollo Regional
"Europa se siente"

Tendencias en ciberseguridad

Josep Albors

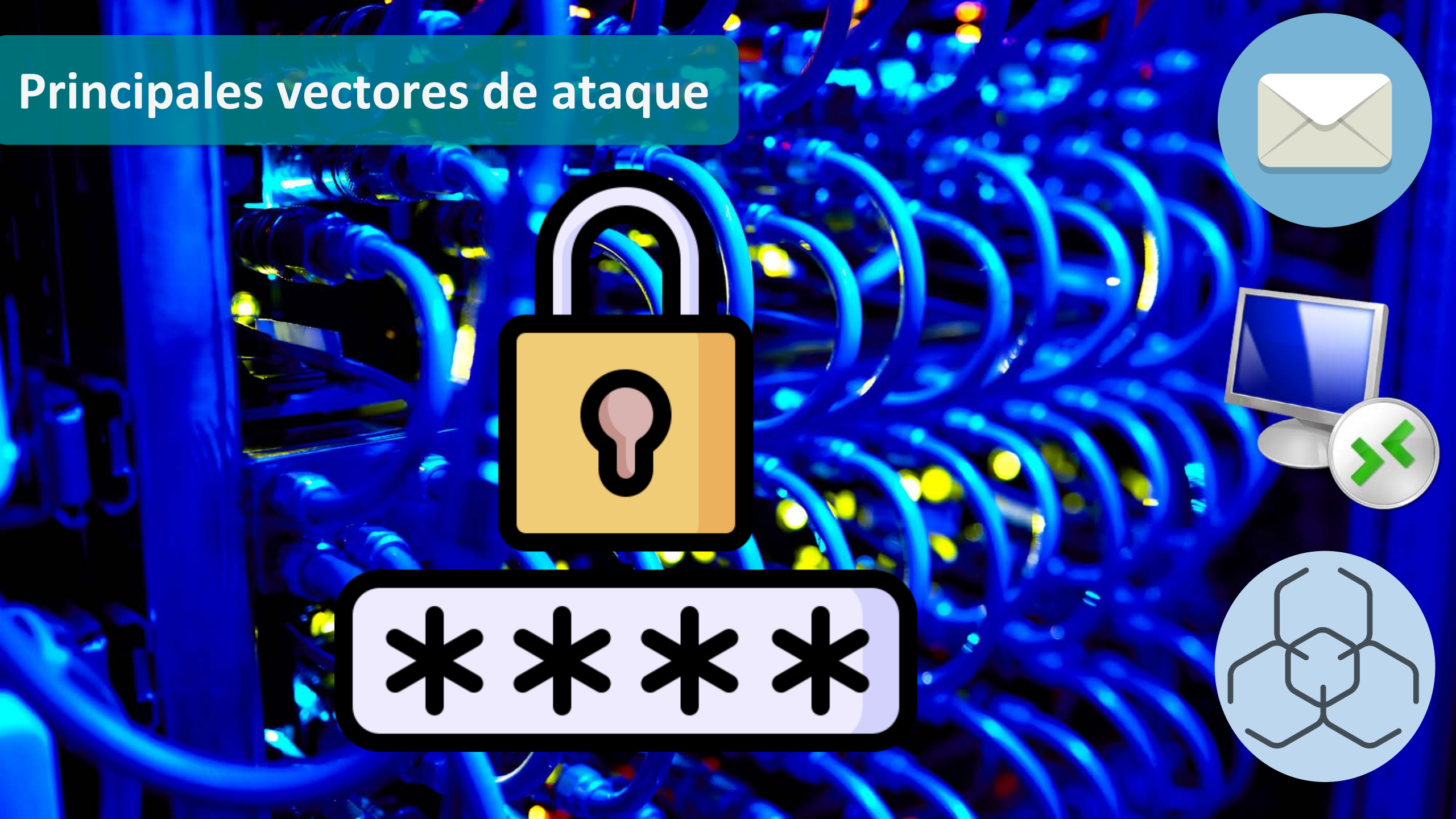
Responsable de investigación y concienciación

ESET Digital Security
Progress. Protected.

Las empresas tienen que proteger **todos sus sistemas**

Los atacantes solo necesitan **un punto de entrada**

Principales vectores de ataque



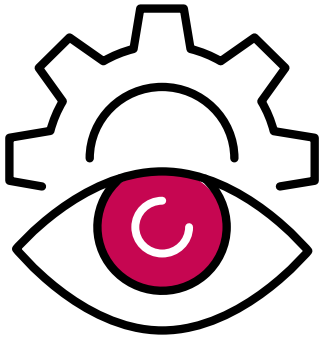
Percepción equivocada

Percepción equivocada

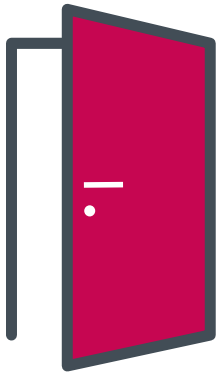
Realidad en España

Infostealers

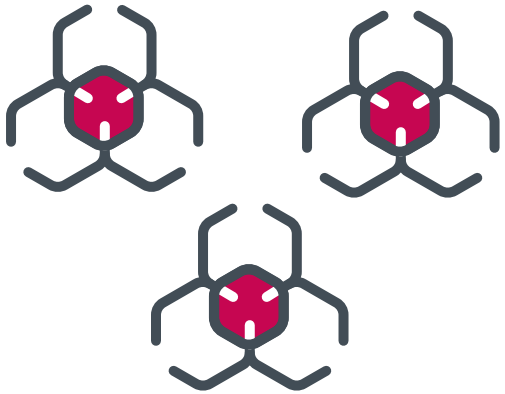
Las RATs actuales



Espionaje y robo de credenciales



Instalación de puertas traseras para permitir accesos remotos



Descarga y ejecución de malware adicional

Casos en España

PROTEGERSE

ÚLTIMAS ALERTAS | CONCIENCIACIÓN | CIBERAMENAZAS

AUMENTO EN ESPAÑA DE LAS DETECCIONES DE INFOSTEALERS QUE USAN CORREOS SUPLANTANDO A TODO TIPO DE EMPRESAS

Josep Albors | 09 Feb, 2023 | Ciberamenazas | No hay comentarios

Durante los últimos días estamos observando un importante aumento en las detecciones de cierto tipo de correos que se encargan de propagar un tipo de malware específico. Nos referimos concretamente a correos que suplantan a todo tipo de empresas e incluso organismos públicos como universidades o la propia Agencia Tributaria, correos que no cesan en su intento de conseguir que los usuarios que los reciban ejecuten los ficheros que llevan adjuntos.

Adjuntos maliciosos en correos sospechosos

Todas estas campañas de correos que venimos observando como han aumentado de intensidad en los últimos días tienen un patrón idéntico, consistente en suplantar a una empresa u organismo reconocido e incitar al receptor del mensaje para que descargue y ejecute el fichero adjunto. Por ejemplo, en uno de los múltiples correos analizados en nuestro laboratorio durante las últimas horas observamos como se suplanta la identidad del banco BBVA, indicando que se adjunta un justificante de pago como gancho para tratar de convencer al usuario.

ES ÉPOCA DE VACACIONES, PERO EL MALWARE ESPECIALIZADO EN EL ROBO DE INFORMACIÓN NO DESCANSA

Josep Albors | 24 Jul, 2023 | Ciberamenazas | No hay comentarios

Segunda quincena de julio. Calor, mucho calor y media España de vacaciones relajándose en la playa, la montaña o donde buenamente pueda. Sin embargo, y aunque las detecciones de amenazas suelen caer durante este periodo, tal y como podemos comprobar en nuestros informes periódicos de amenazas dirigidas a España, hay algunos delincuentes que no descansan ni durante las vacaciones.

Facturas, pagos y otras excusas para hacernos caer en la trampa

Sabiendo que todo aquello relacionado con dinero y, especialmente, lo que toque nuestra cartera, suele despertar especial interés en el usuario medio español, no es de extrañar que estos asuntos sean los más utilizados en las plantillas de los correos que preparan los delincuentes para tratar de conseguir nuevas víctimas.

Estos correos maliciosos pueden ser más o menos genéricos y estar más o menos elaborados, tal y como hemos estado viendo durante estos últimos años. Sin embargo, todos tienen la misma finalidad, que no es otra que conseguir engañar al receptor de este mensaje para que descargue y ejecute el fichero adjunto o pulse sobre el enlace proporcionado. Veamos dos ejemplos recientes analizados en nuestro laboratorio.

CUIDADO CON LA FALSA TRANSFERENCIA DEL SANTANDER QUE PUEDE TRAERNOS DESAGRADABLES SORPRESAS

Josep Albors | 08 Nov, 2023 | Ciberamenazas | No hay comentarios

Cuando somos responsables de gestionar pagos y cobros en una empresa es habitual recibir varios correos electrónicos, incluso decenas de ellos, al día que requieren de nuestra atención. Esto es algo de lo que los delincuentes tratan de aprovecharse continuamente, confiando en que algún usuario abrirá alguno de los ficheros adjuntos o enlaces que incluyen en correos que se hacen pasar por otras bancarias, organismos oficiales o, como en este caso, entidades bancarias.

Ejemplos campañas Agent Tesla

[se encontró la amenaza ESET LiveGuard Troyano] AEAT - Aviso de Notificación

Agencia Tributaria <agenciatributaria@correo.aeat.es>

Respond

Caducidad de tu Certificado FNMT.

Notificaciones FNMT AC Usuarios <ac.usuarios@fnmt.es>

Responder a todos

Location: /

olders

Agencia Tributaria.rar

Name	Size	Type	Date Modified
Agencia Tributaria.exe	1.0 MB	DOS/Windows executable	17 October 2023, 11:11

Location: /

olders

Certificado- FNMT.rar

Name	Size	Type	Date Modified
Certificado- FNMT.exe	1.0 MB	DOS/Windows executable	17 October 2023, 10:01

electrónicas (notificacion.060.es).

Un saludo.

Agradecemos sinceramente su confianza en nuestros servicios.

Ejemplos campañas Agent Tesla

[REGLA] [se encontró la amenaza Suspicious Object] Su DHL Notificación de envío: 00782149

Alex Menjivar (DHL)<alex.menjivar@dhl.com>

Ayer, 15:10

Responder a todos

Factura detalles_00537_...

49 KB

descargar

[REGLA] [se encontró la amenaza una variante de MSIL/Kryptik_AGen.BVD Troyano] Aviso de pago de fecha 30.1.2024

info@caixabank.es

Hoy, 0:41

Responder a todos

CaixaBank _ banca digit...

Servicio: P
Piezas: 2
PERSONAL: Ref.
Descripción: FACTURA COMERCIAL Y CONOCIMIENTO DE ATERRIZAJE ETC

Saludos

¡Gracias por realizar el envío con DHL Express!
Deutsche Post DHL, el grupo de correo y logística
2024 @ DHL INTERNACIONAL GMBH.....
CORREO ELECTRÓNICO..DHL @ DELIVERY.COm

Gracias por confiar en nosotros.

info@caixabank.es

Atentamente CaixaBank Payments & Consumer

Ejemplos campañas Formbook

[SPAM] DHL Shipment Notification : 716158433805092022

DHL® GLOBAL FORWARDING<leo.nav@azarpajouh.com>

Responder a todos

Dear [redacted]

Notification for shipment event group "Clearance event" for 22 **Sept. 2022**

AWB Number: 7575544723
Pickup Date: 2022-09-22 15:52:00
Service: P
Pieces: 6
Cust. Ref: S/C#SD2250194
Description: PAPER LABEL-HS#48211000 MADE IN CHINA

Attached is the Original Shipping documents and BL as assigned to be deliver to you.

Further Details - Awaiting authorization of/or advance duty payment from customer.

Next Steps - Clearance processing will proceed as soon as authorization or pre-payment is receive

Importer is advised to contact DHL Customer Service if further details are required.

A DHL representative shall attempt to contact the importer or shipper if required.

[se encontró la amenaza una variante de MSIL/GenKryptik.GAIV Troyano] TNT Express delivery Consignment Notification 811470484778

TNT Import<service@tnt.com>

Ayer, 9:08

Recipients<service@tnt.com>

Responder a todos

[se encontró la amenaza una variante de MSIL/Kryptik.AIJA Troyano] [ESET-SPAM] Aviso de Transferencia Realizada

BSOnline.Empresa@bancsabadell.com

Ayer, 15:50

Responder a todos

prueba de transferencia ...
721 KB

Servicio de notificación de transferencias

Tenemos el placer de informarle que hoy dia 16.03.2023, hemos realizado una orden de transferencia a su favor a través de Banca a Distancia de Banco Sabadell a petición de nuestro cliente.

Adjuntamos el comprobante de transferencia para su confirmación.

Contacte con nosotros: telefono**963 085 000** contactoSolicite una cita previa.

También le atenderemos:

facebook twitter google+

Certificado de seguridad:
certificate

Este mensaje se ha generado a peticion del Ordenante de la transferencia, conforme a los datos y contenido facilitados por el mismo, para su envio a través del servicio de avisos del Banco de Sabadell, S.A. (www.bancsabadell.com). Los datos personales que se indican son utilizados de forma estrictamente confidencial con el único fin de prestar el indicado servicio y con las garantías del artículo 12 de la Ley Orgánica 15/1999 de Protección de Datos de Carácter Personal. Tratándose de un servicio de comunicación automática, para cualquier consulta, objeción o comentario deberá dirigirse directamente al propio Ordenante.

Para acceder, cancelar o rectificar sus datos o la dirección de correo electrónico en la que quiere recibir este tipo de información puede enviar una carta por correo postal o pasar por cualquiera de nuestras oficinas. Si no desea recibir más información comercial por correo electrónico, simplemente haga clic aquí.

Banco de Sabadell, S.A. Pl. Sant Roc, 20, 08201 Sabadell. Inscrito en el Registro Mercantil de Barcelona, tomo 20093, hoja B-1561, NIF A08000143. Dirección de correo electrónico: info@bancsabadell.com

[SPAM] [se encontró la amenaza VBS/Agent.QMG Troyano] Confirming - Aviso de pago

Factoring y Confirming - Grupo Santander<fycout.gruposantander.es@autocentrosbernardino.es>

Hoy, 9:05

Responder a todos

Para ayudar a proteger tu privacidad, parte del contenido de este mensaje se ha bloqueado. Para volver a habilitar las características bloqueadas, haga clic aquí.

Para mostrar siempre el contenido de este remitente, haga clic aquí.

5573_Confirming_68573...
708 KB

descargar

Muy Sres. nuestros: Se adjunta carta de liquidación. Atentamente, Santander Factoring y Confirming S.A. EFC Proveedor: TOU-579308 RefMailJ: #198915919##

Por razones de seguridad le rogamos no conteste a este correo electrónico. Para no ser víctima de un fraude siga estos para protegerse.
consejos de Seguridad online

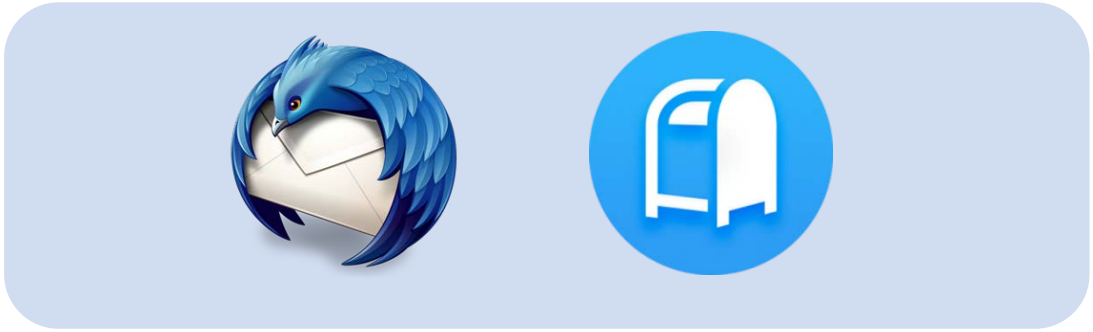
For security reasons, please do not reply to this email. To avoid becoming a victim of fraud, follow these yourself.
online Security tips to protect

Santander Factoring y Confirming S.A. E.F.C. Sociedad Unipersonal inscrita en el R.M. de Madrid, Hoja 70685-1 Folio Tomo 1001, Sección 3ªA Inscripción 1º C.I.F. A-78287562

Robo de credenciales

Navegadores de Internet

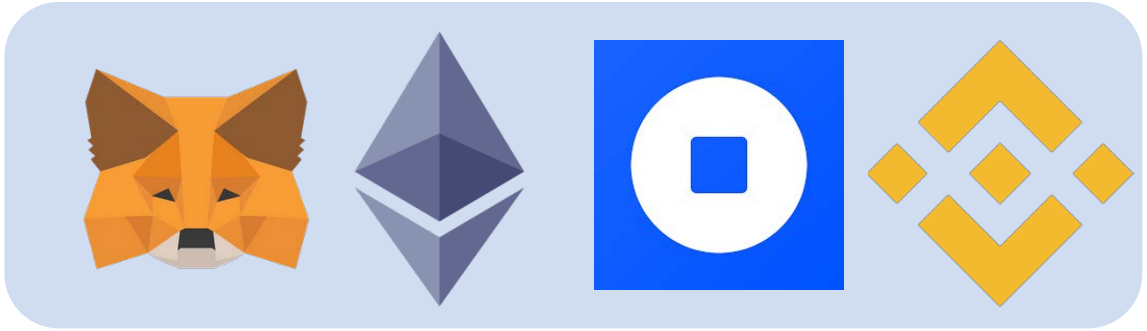
Clientes de correo



Clientes FTP y VPN

Videojuegos y mensajería

Carteras criptomonedas



Amenazas por Email

Explotación de vulnerabilidades antiguas

[se encontró la amenaza probablemente una variante de Win32/Exploit.CVE-2017-11882.F Troyano] RE: Cotización de precio

Elisabeth
Hoy, 5:22

Responder a todos

especificación.xlsx
224 KB

descargar

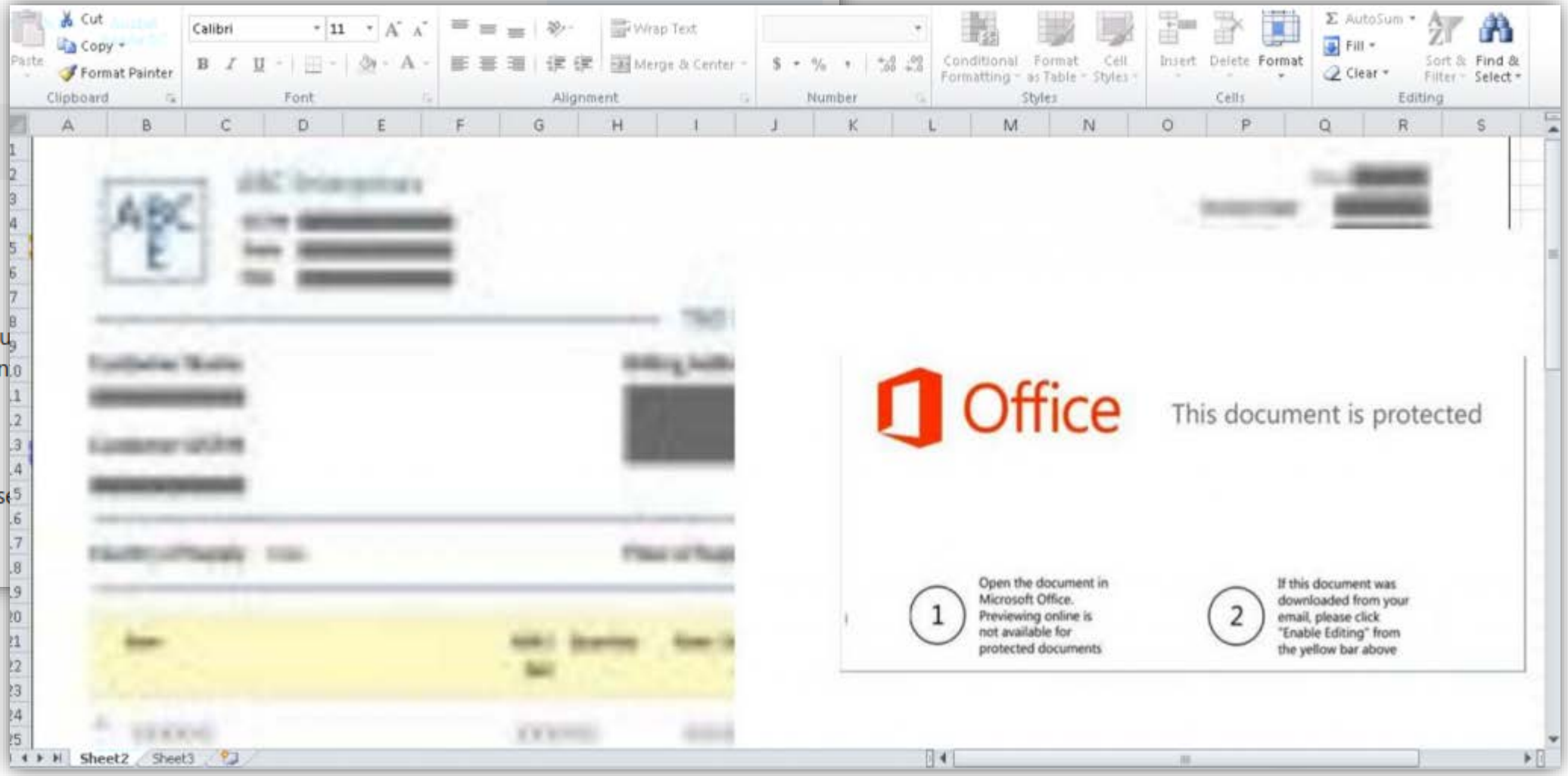
¡Buenos días!

Indique su lista de precios actu
para las especificaciones adjun

espero su respuesta urgente.

Gracias de antemano y les dese

Saludos



Alternativas al uso malicioso de las macros

[SPAM] [ESET-SPAM] Factura pendiente de pago

GRUPO SOCI SLU <infoport@mythicalsportwear.com>

Responder a todos

Hoy, 11:52

Ventas ESET

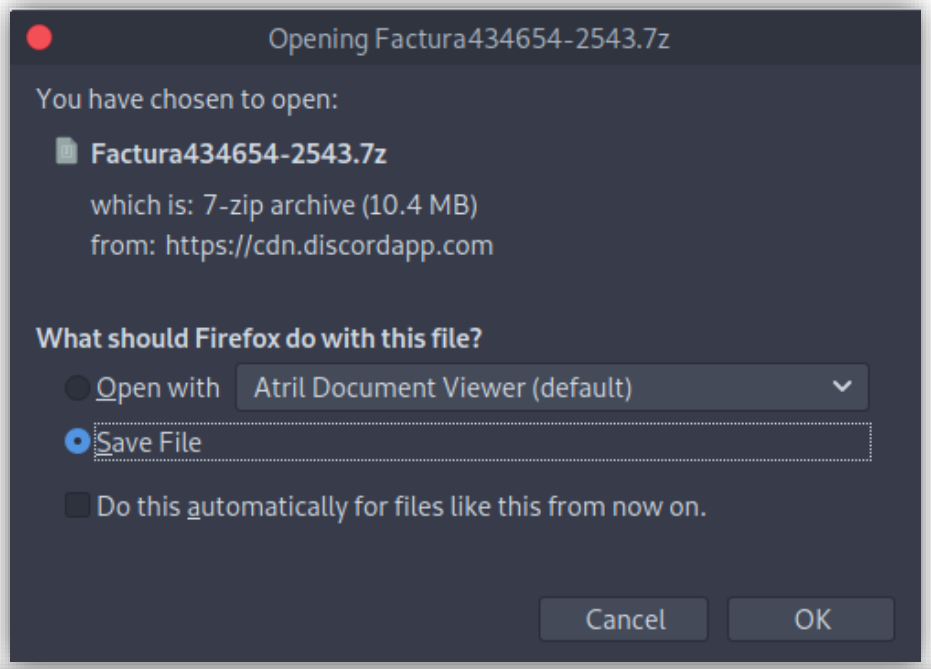
Factura102947312.pdf
80 KB

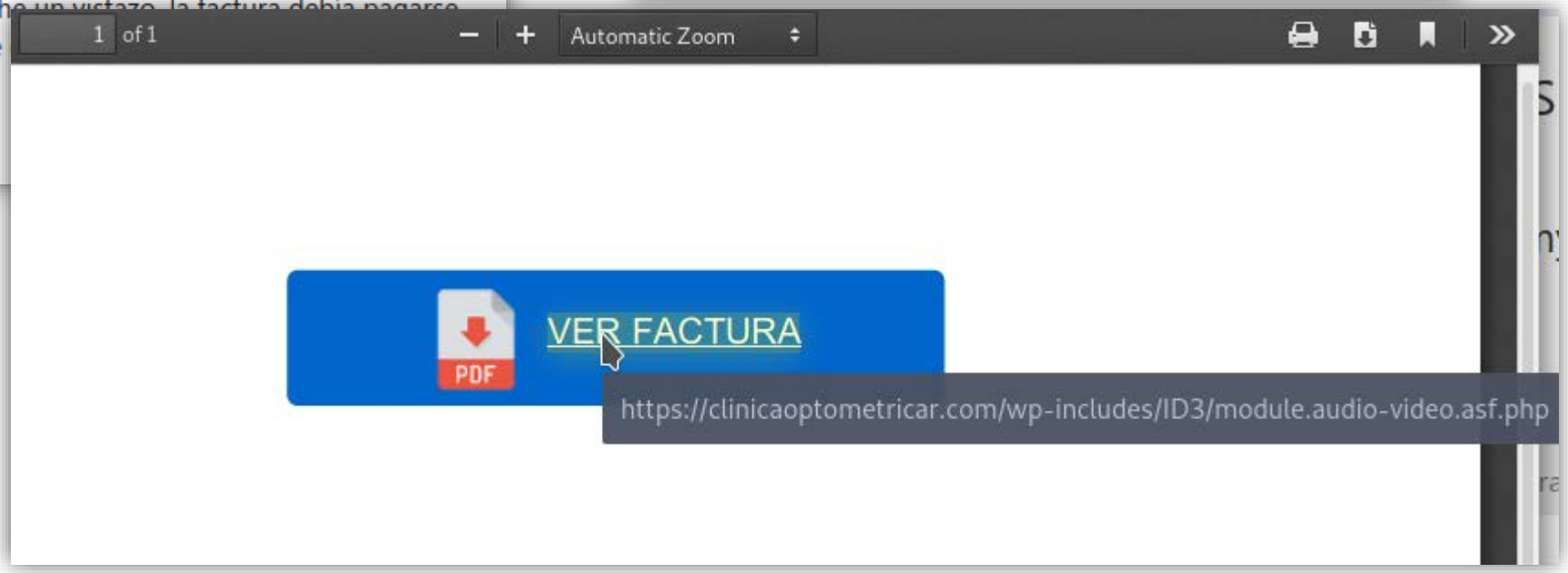
descargar

Buenas dia,

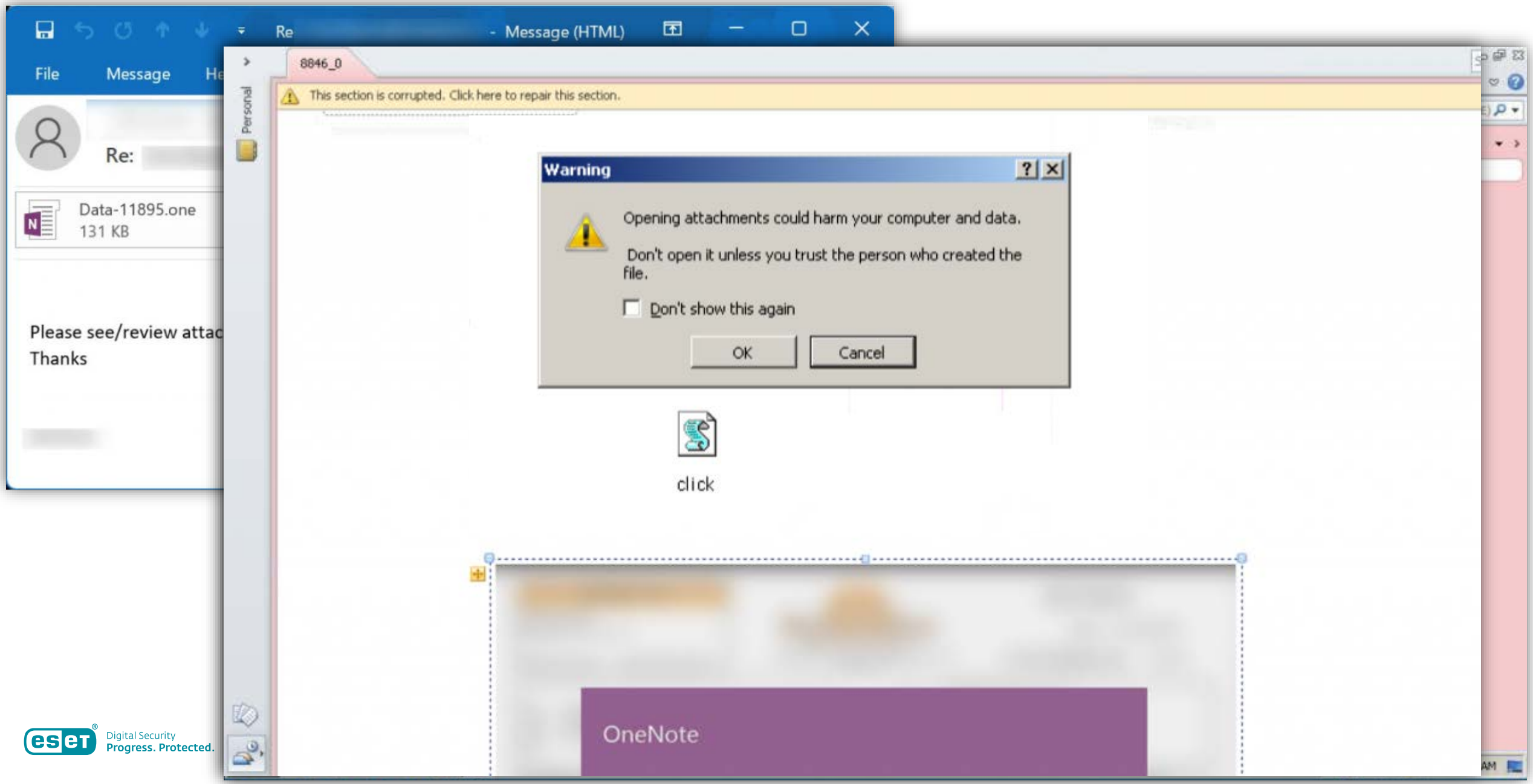
Adjunto tenéis la factura que no está pagada. Por favor, eche un vistazo, la factura debía pagarse hace 5 días. Si ya realizó el pago, envíenos el comprobante

Departamento de facturación.





Alternativas al uso malicioso de las macros



Phishing

Phishing dirigido a empresas

[SPAM] [ESET-SPAM] Human Resources Notification Ref: 10262022

HR Department<cla.dic@disdoni.com>
Hoy, 7:02
Ayuda ESET

Responder a todos

Requested by : HR Department
Position : Director of Human Resources

Good day ayuda ,

Kindly check staff memo referring to the
for our annual open vacation plan.

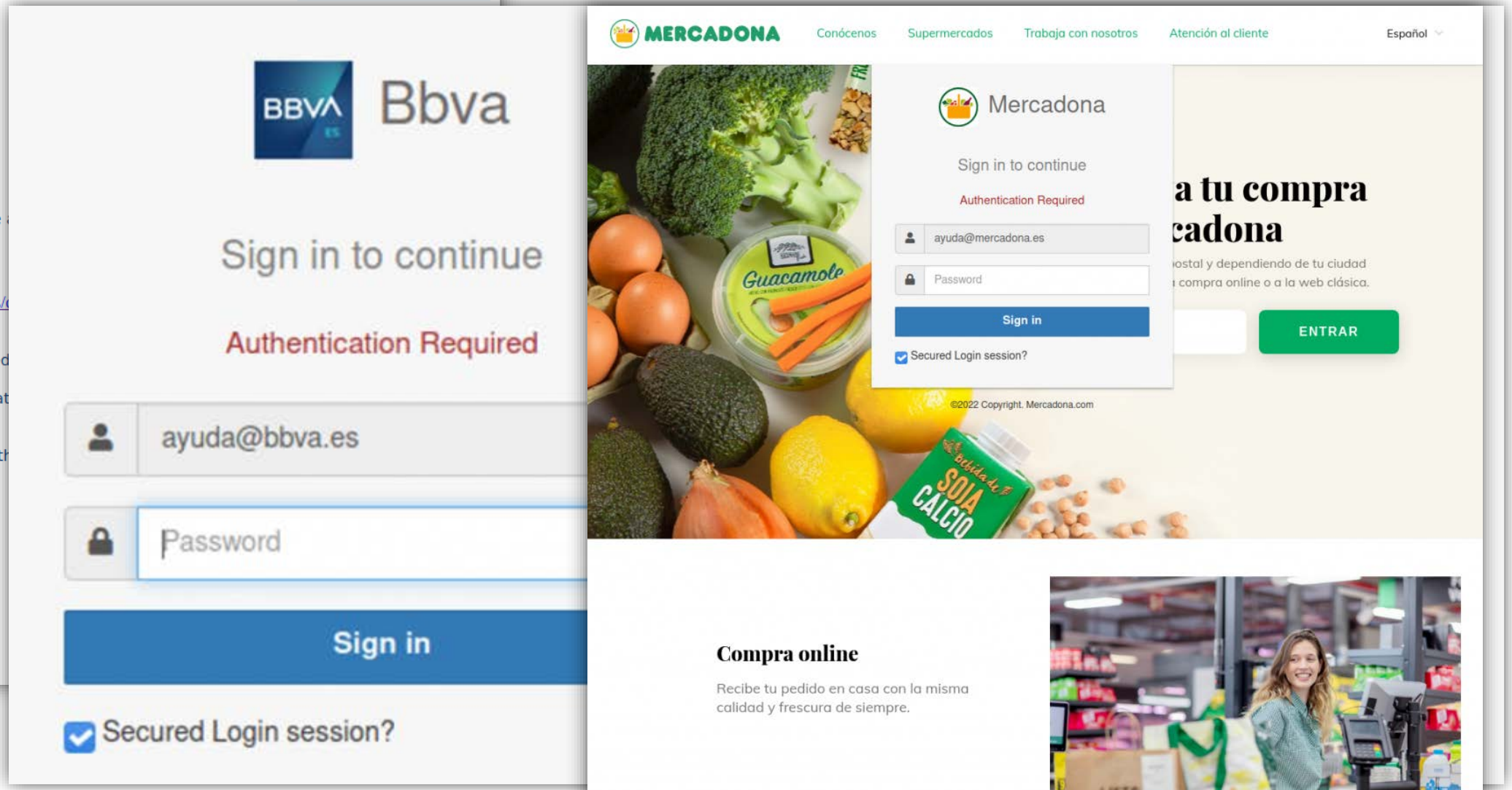
ticketfind-and-update.staff-information.eset.es/

Please do note that all names highlighted

Marked in yellow color indicates staff stat
on/before the end of the month.

Please let me know,should you have furth

Thanks & Regards,
Director of Human Resources
HR Manager
eset.es
Email :- hr@eset.es
Web :- https://www.eset.es



eset Digital Security
Progress. Protected.

Suplantación de organismos gubernamentales

[SPAM] [ESET-SPAM] Aviso de notificación de la Agencia Tributaria
[redacted]

AgenciaTributaria@correo.aeat.es<noreply@correo.aeat.e
Ayer, 14:05
[redacted]

ESTE EMAIL SE CORRESPONDE CON UN AVISO DE UNA NOTIFICACIÓN

Le informamos que está disponible una nueva notificación para msanchez

- Titular[redacted]
- Organismo emisor: Agencia Estatal de Administración Tributaria, con
- Identificador: 51452666411e4bf42a89
- Concepto: Notificación administrativa (Serie SF0249)
- Vínculo: Titular

Puede acceder a esta notificación en la Dirección Electrónica Habilitada Ún
General, disponible en: https://agenciatributaria.gob.es

Le facilitamos un enlace directo a la notificación.

De acuerdo con lo previsto en los artículos 41 y 43 de la Ley 39/2015, de 1
Administrativo Común de las Administraciones Públicas, la aceptación de l
notificación o bien la presunción de rechazo por no haber accedido a la nc
a disposición, dará por efectuado el trámite de notificación y se continuará

Puede recibir esta notificación por distintas vías electrónicas o incluso en p
contenido de esta notificación por más de una de estas vías, sepa que los
empiezan a contar desde la fecha en que se produzca su primer acceso.

Gobierno de España

https://appbarcelona.com/recovery/store.php?aGwLBnwAk=[redacted]

agenciatributaria.bz/hrhhgnxfqy/main.php?&id=6368882&utm_tem=91744&utm_cmpaign=login&utm_mdium=7...

GOBIERNO DE ESPAÑA · MINISTERIO DE HACIENDA Y FUNCIÓN PÚBLICA

ÁREA PERSONAL · ES

Dirección de correo electrónico
Escriba su dirección de correo electrónico.

Contraseña
Escriba su contraseña de correo electrónico.

Entrar

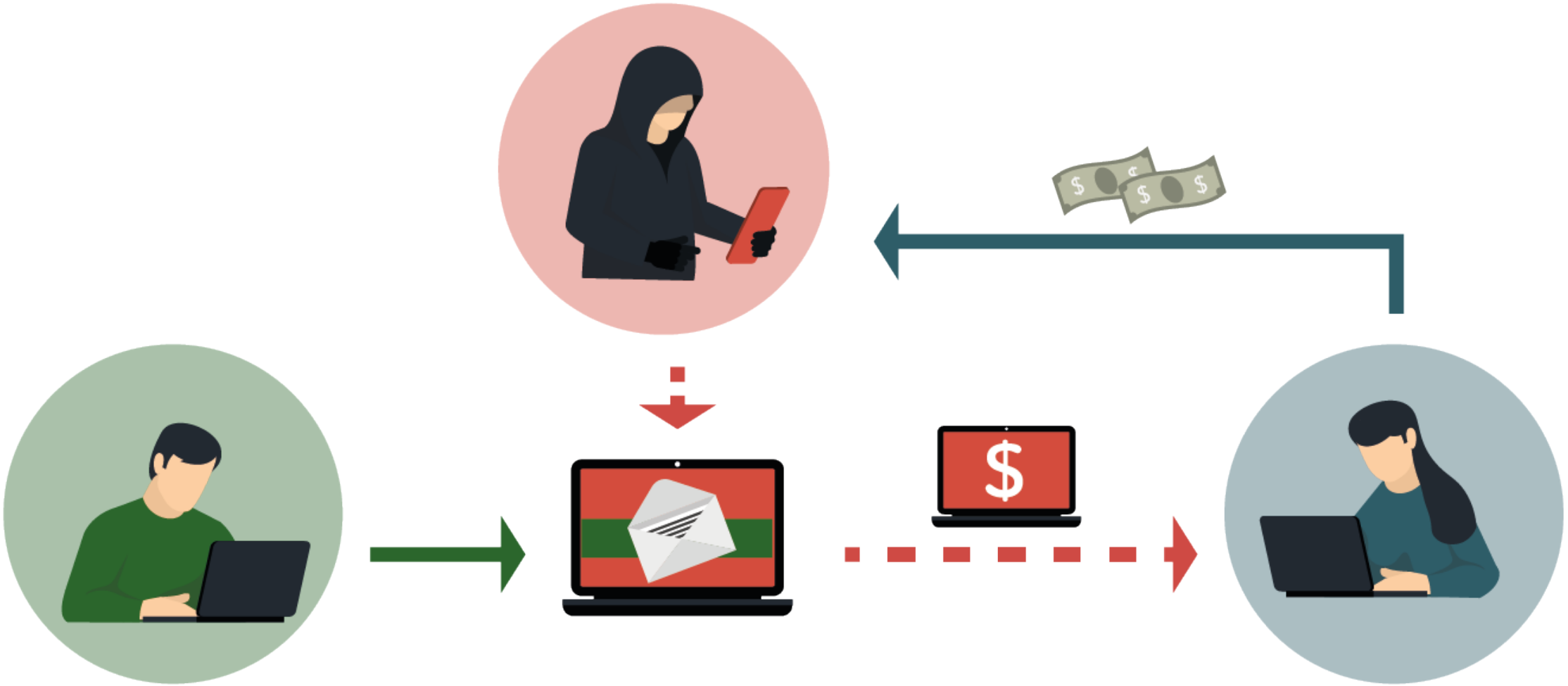
Agencia Tributaria
- Accesibilidad
- Aviso de seguridad
- Aviso legal
- Validación del certificado de sede
- Protección de datos
- Política lingüística
- Estructura y navegación en la sede electrónica

Contacta con nosotros
- Teléfonos de interés
- Buscador de oficinas
- Cita previa
- Buzones de sugerencias
- Denuncias
- Suscripción newsletter
- Suscripción RSS

Ayuda
- Buscar
- Consultas informáticas
- Diseños de registro
- Horario de interrupciones de sede
- Manuales, vídeos y folletos
- Simuladores
- Todas las ayudas

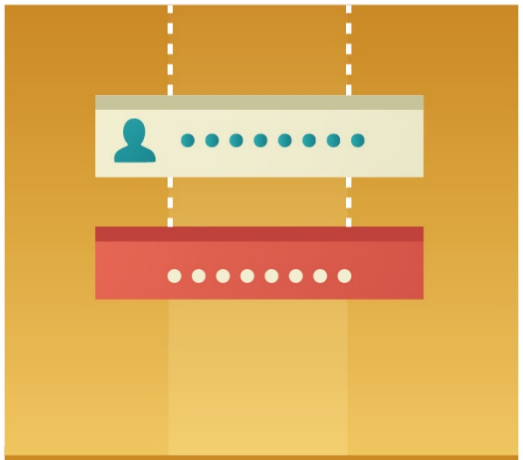
Enlaces de interés
- Ministerio de Hacienda y Función Pública
- Fiscalidad autonómica y local
- Consejo para la Defensa del Contribuyente
- Punto de Acceso General
- Portal de la transparencia
- Otros enlaces de interés

FRAUDE DE CEO



Fraude del CEO

¿QUÉ ES BUSINESS EMAIL COMPROMISE (BEC)?



ACCESO ILEGAL

Los delincuentes acceden a los dispositivos o sistemas de las víctimas mediante piratería, sitios web de phishing o software malicioso, y posteriormente engañan a la víctima para que realice una transferencia de dinero a su cuenta bancaria.

INGENIERÍA SOCIAL

Los delincuentes eligen a sus víctimas basándose en la información que estas comparten en las plataformas de medios sociales.

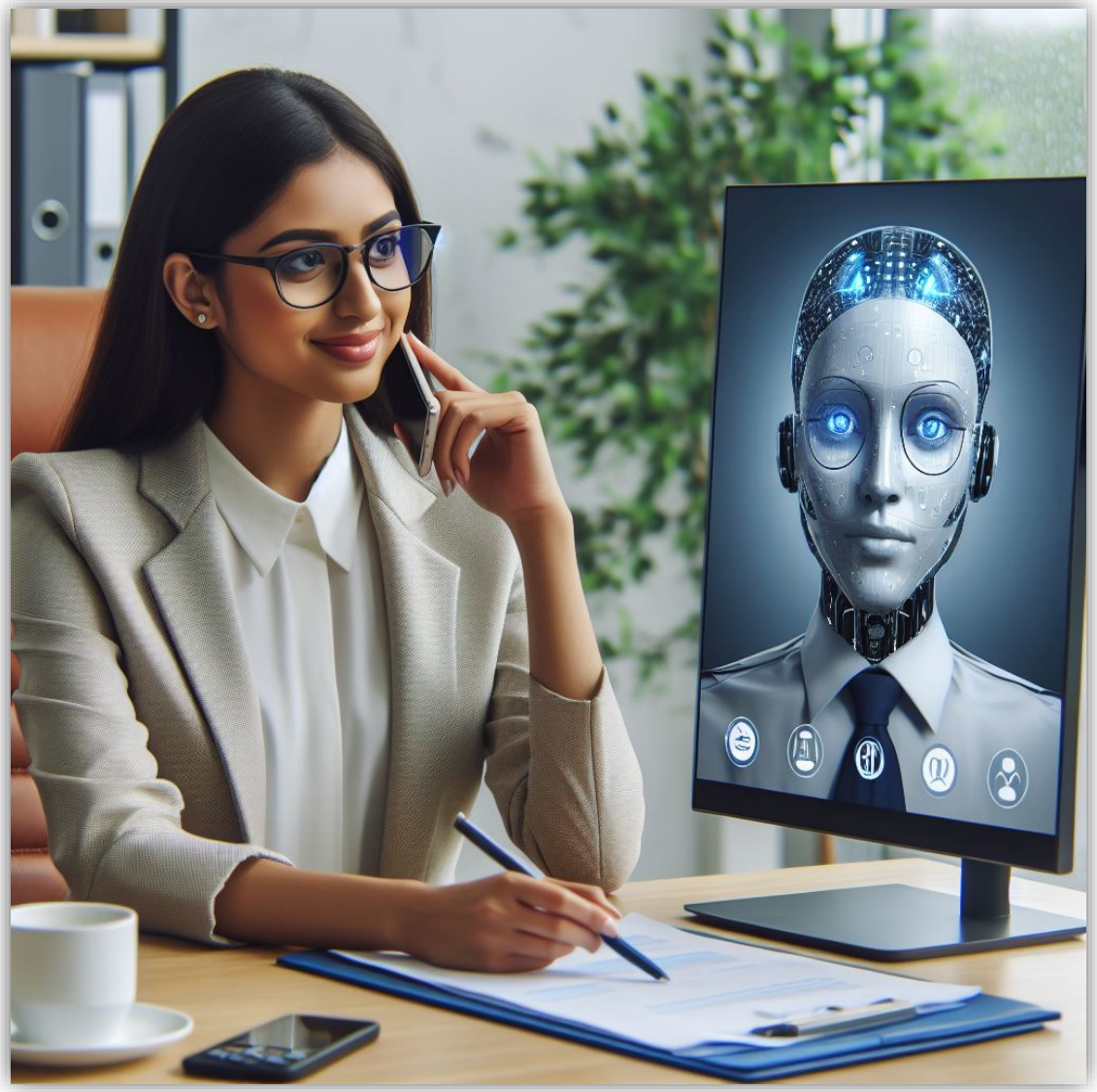
SOLICITUDES URGENTES

El delincuente se hace pasar por un proveedor solicitando un pago urgente o el cambio de la información bancaria, o por un empleado de alto nivel en la empresa con autoridad para autorizar pagos.

#BECareful

INTERPOL

Fraude del CEO con IA



Objetivos de los atacantes

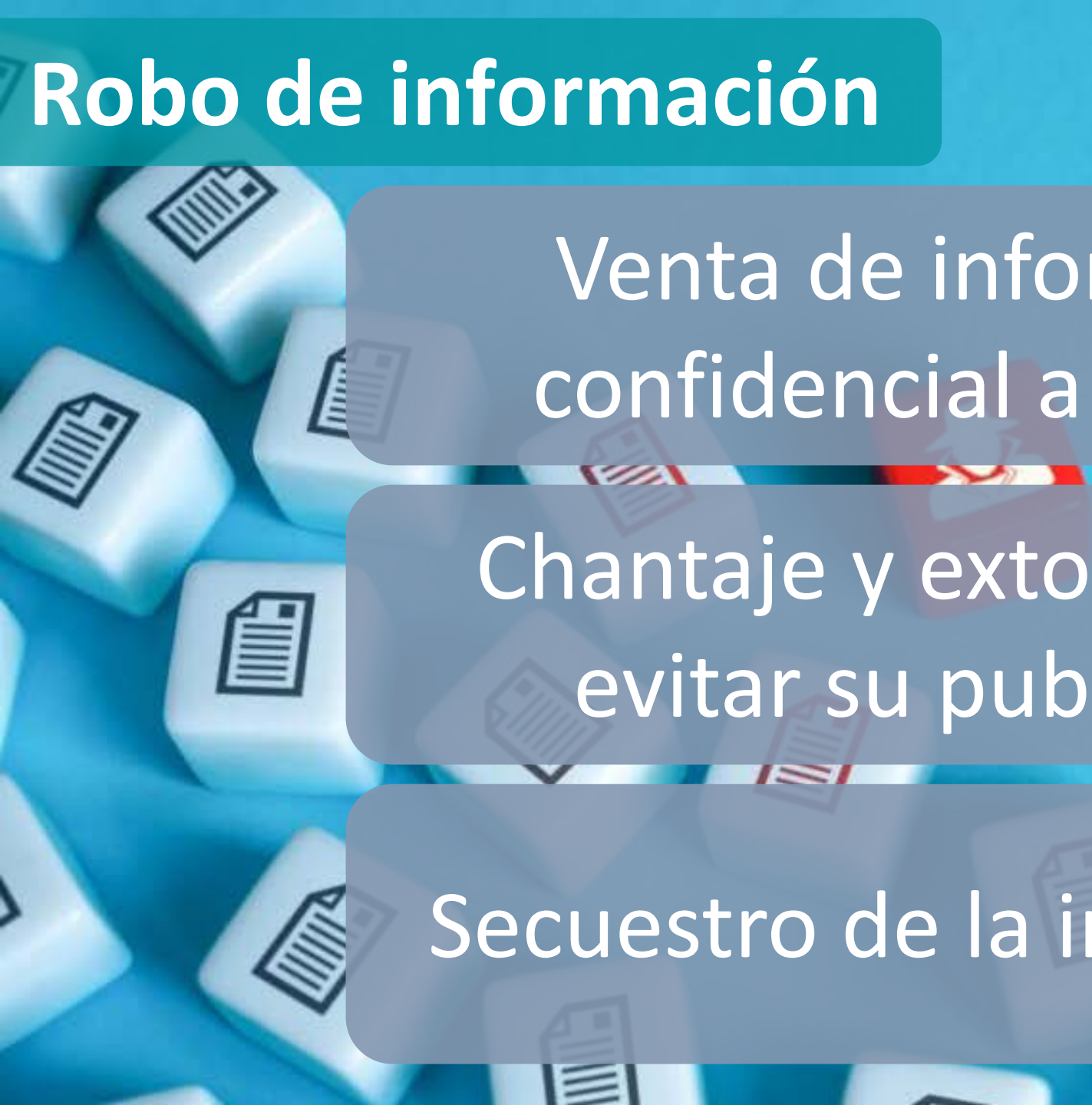
Benefico económico directo

Robo de credenciales de acceso a la banca online

Robo de datos de tarjetas de crédito

Recepción de transferencias realizadas por engaño

Robo de información



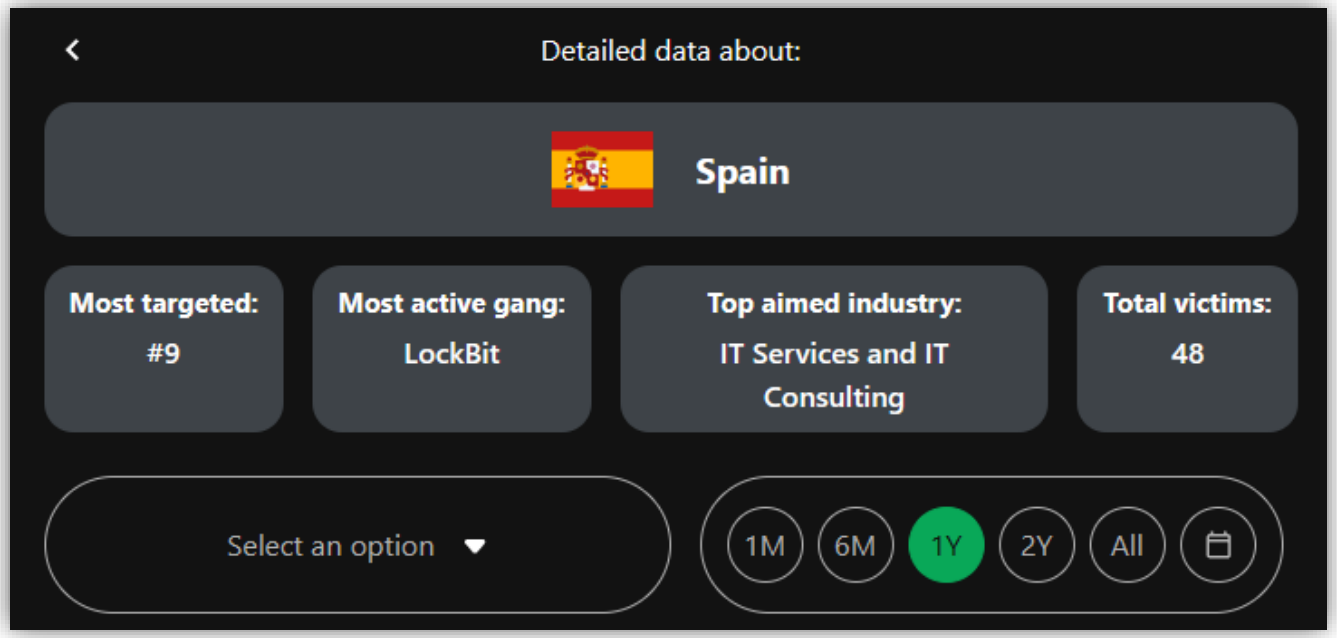
Venta de información confidencial a terceros

Chantaje y extorsión para evitar su publicación

Secuestro de la información


RANSOM!
Your files have been encrypted

Ransomware en España



¿Cómo funciona el "ransomware" que ha sufrido el Ayuntamiento de Sevilla?

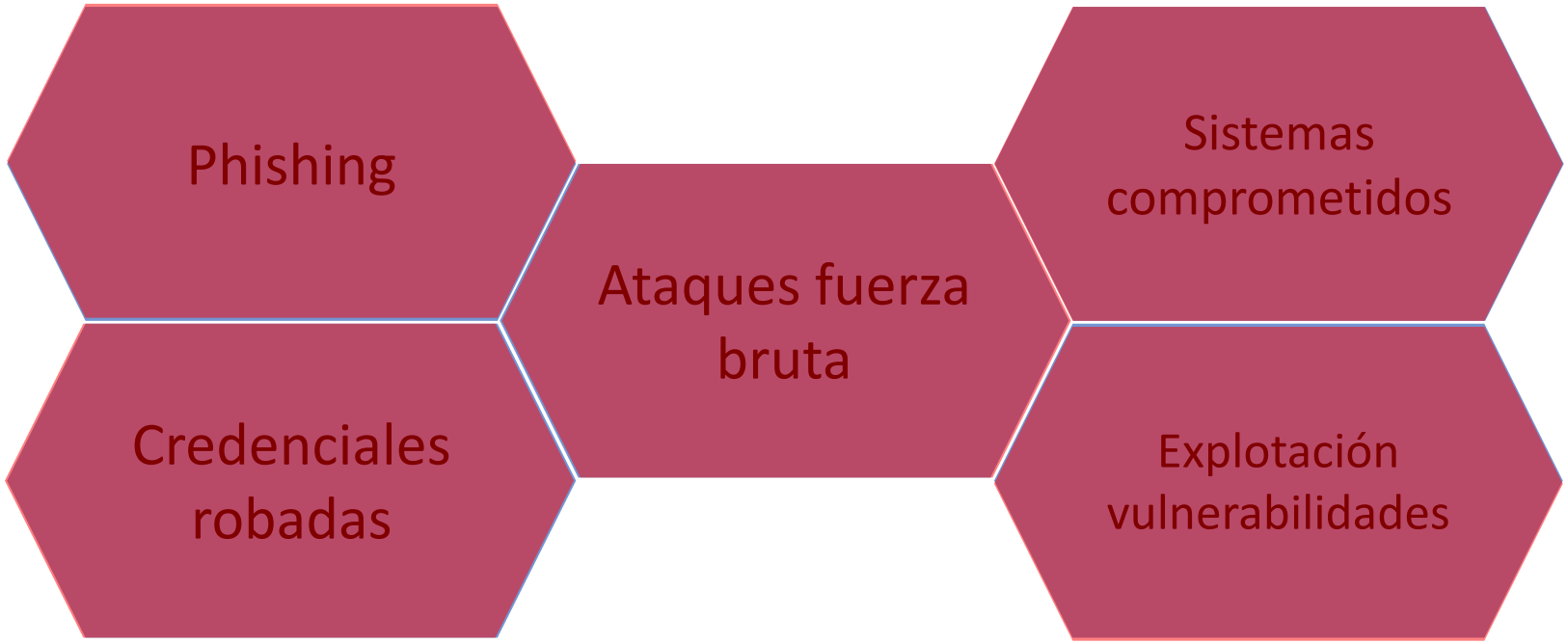
Este tipo de programa malicioso llega a las víctimas por medio de un correo electrónico en el que se engaña a la persona que lo recibe

▲Un grupo de hackers argelinos puede estar detrás de uno de los ciberataques jmz

AGENCIA EFE

Madrid Creada: 06.09.2023 19:21
Última actualización: 06.09.2023 19:21

Ransomware: acceso inicial



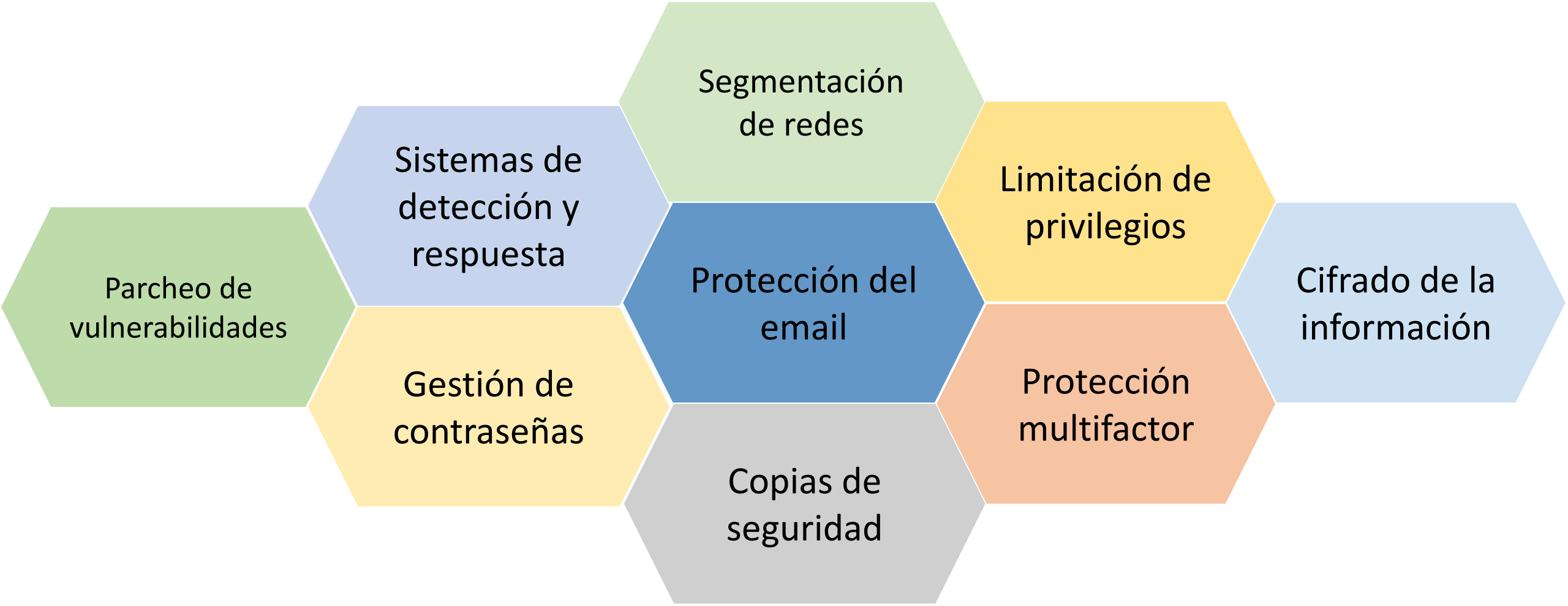
Vectores de ataque clásicos y nuevos

Aprovechamiento de vulnerabilidades

Uso de herramientas del sistema

Conocimiento del objetivo

Medidas de mitigación



No cargues con todo

Josep Albors

Responsable de investigación y concienciación
ESET España

@josepalbors

mypublicinbox.com/JosepAlbors

Digital Security
Progress. Protected.

Tendencias en Ciberseguridad

Tecnologia para proteger nuestros activos

Carlos Tortosa
Responsable grandes cuentas

ESET® Digital Security
Progress. Protected.

Acerca de ESET

+ 30 años en el mercado

Empresa privada, sin deudas

Siempre enfocados en la tecnología

Principal proveedor de la Unión Europea

Creciendo año tras año desde su inicio

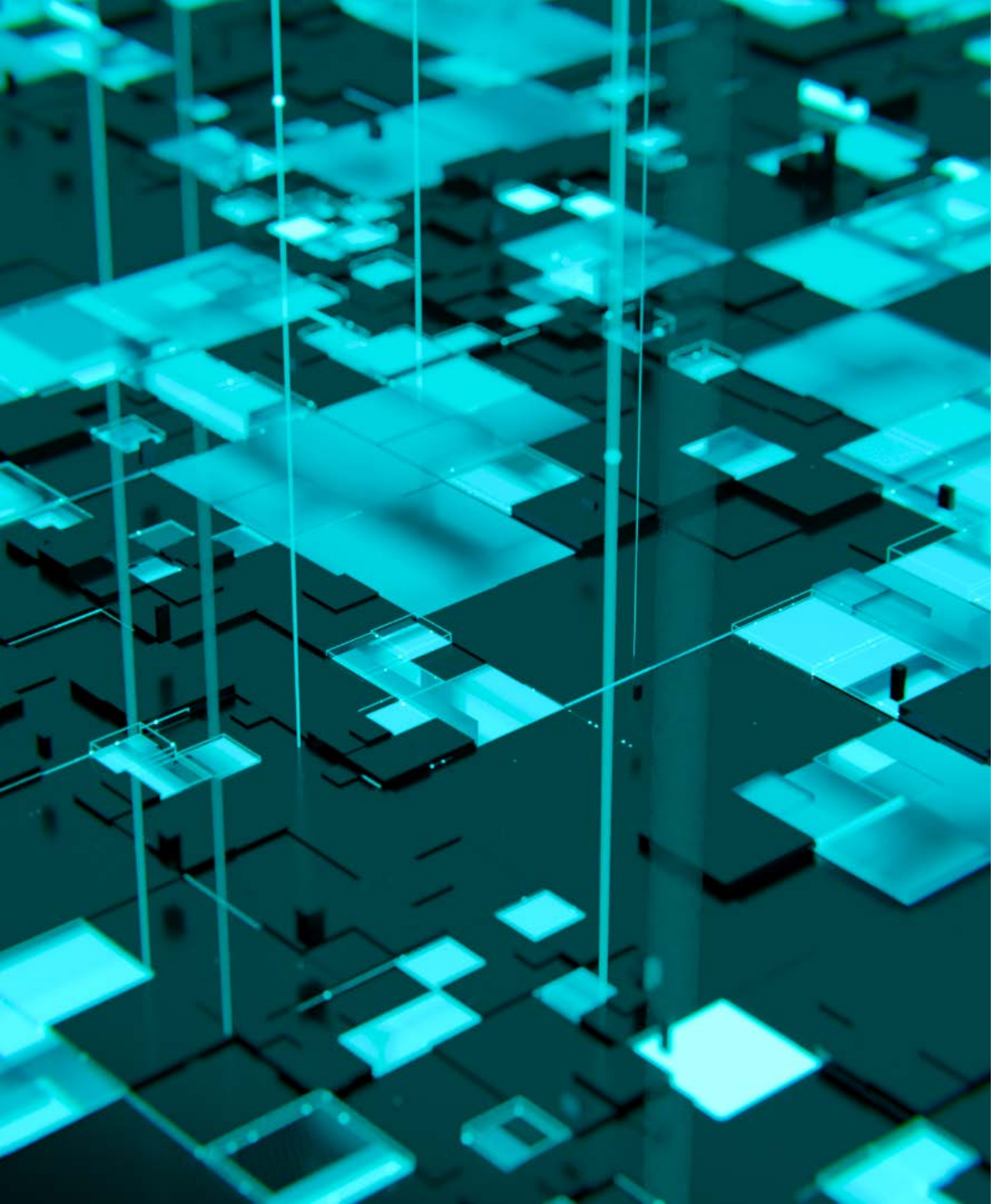
Propiedad de los fundadores originales

Valores

sólidos

Progress. Protected.


SERVICIOS PROFESIONALES

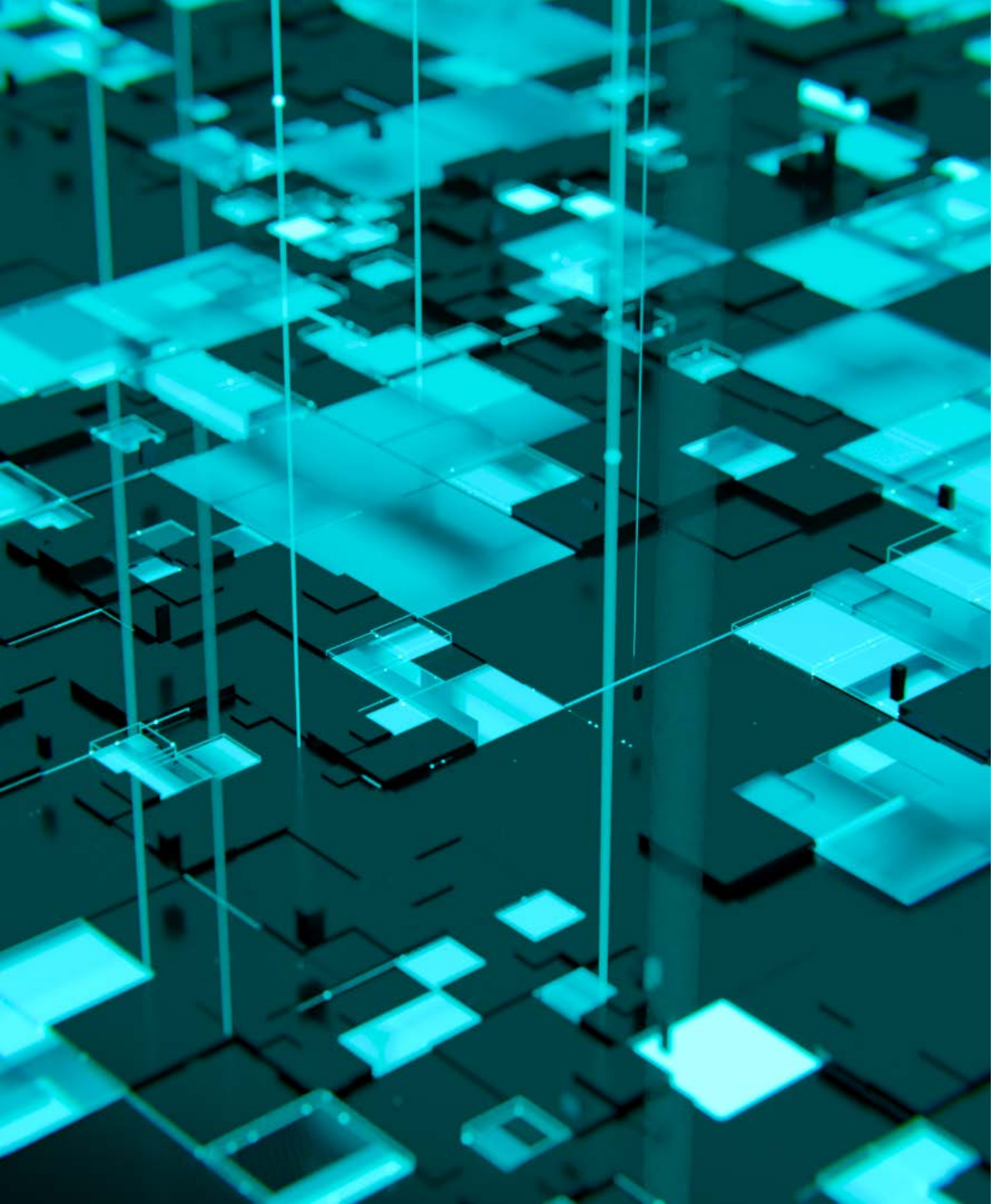


Instalación

Instala, migra o actualiza remotamente un producto específico por parte de nuestros técnicos de soporte certificados.

ESET soporte Premium

Acceso 365/24/7 a especialistas en atención al cliente con años de experiencia en seguridad de IT.



Configuración

Nuestros especialistas realizan una configuración, revisión y optimización de los productos contratados con ESET.

Monitorización

Monitorización y gestión profesional y constante (24x7) de las alertas de seguridad de las soluciones ESET.

“Es prácticamente seguro que seremos objetivo de algún tipo de ciberataque. Por eso, es fundamental que pongamos todo lo que podamos de nuestra parte para hacer que los atacantes sufran lo indecible y que desistan de sus intenciones”

GRACIAS

Carlos Tortosa
Key Account Director
ctortosa@eset.es

Digital Security
Progress. Protected.