Contenido

Malware

Malware eo ?Malicious software?, se trata de programas maliciosos cuya función es dañar un sistema o causar un mal funcionamiento. Dentro de este grupo podemos encontrar numerosos términos entre los cuales están:

- **Virus:** Los Virus Informáticos son malwares que infectan a otros archivos del sistema con la intención de modificarlo o dañarlo.
- **Adware:** El adware es un software que despliega publicidad de distintos productos o servicios.
- **Backdoors o puertas traseras:** Estos programas son diseñados para abrir una ?puerta trasera? en nuestro sistema de modo tal de permitir al creador de esta aplicación tener acceso al sistema y hacer lo que desee con él. El objetivo es lograr una gran cantidad de computadoras infectadas para disponer de ellos libremente hasta el punto de formas redes.
- **Keylogger:** este programa, usado como malware, capta las pulsaciones realizadas en el teclado y las guarda en un fichero que posteriormente envía a través de Internet. Se usa para robar contraseñas.

- **Phishing:** o suplantación de identidad. Para ello se requiere conocer los datos los datos de la victima: usuario, contraseña, nº de cuenta, etc. Los métodos para conseguir estos datos y pueden involucrar un keylogger o correos fraudulentos o incluso una llamada telefónica requiriendo nuestros datos.

- **Spam:** o correo basura. Suele ser correo con fines publicitarios y remitente anónimo o desconocido, enviado normalmente en grandes cantidades. No causan daños ocultos pero si molestias en los usuarios. Normalmente se asocia el spam a otras técnicas como phishing para recabar datos a gran escala.

- **Troyano:** se presenta al usuario como un programa útil e inofensivo pero que abre una puerta trasera que permite al atacante tomar control de la máquina. Normalmente su presencia pasa inadvertida al usuario, pero no a los antivirus.

- **Ransomware:** es un malwatre malintencionado que restringe el acceso a determinadas partes o archivos del sistema infectado, y pide un rescate a cambio de quitar esta restricción, como el muy conocido *virus de la policia*. Algunos tipos de ransomware cifran los archivos del sistema operativo inutilizando el dispositivo y coaccionando al usuario a pagar el rescate. Estos últimos se han conocido como 'Cryptolockers'.

- **Botnet:** Una botnet es una red de equipos infectados por códigos maliciosos, que son controlados por un atacante, disponiendo de sus recursos para que trabajen de forma conjunta y distribuida. Cuando una computadora ha sido afectado por un malware de este tipo, se dice que es un equipo es un robot o zombi.

Correos Fraudulentos

El correo es una de las vías más importantes para que nuestro PC sea atacado. Bien siendo victimas de virus, malware o phising. El propósito de este artículo es ir recopilando a modo de muestra ejemplos de correos fraudulentos y la manera de identificarlos. Cómo el ingenio de los atacantes se incrementa con el tiempo iremos actualizando la página para que sirva de referencia de correos antiguos y de los últimos que se vayan recibiendo.

Es posible que recibáis correos en los que se os pide pulsar en un enlace o bien aportar datos de vuestras cuentas de correo u otros datos confidenciales. Son mensajes fraudulentos, no importa quien aparezca como remitente. Os recordamos que **el servicio de informática, ni ninguna entidad pública pedirá vuestra contraseña ni que pulséis sobre ningún enlace, a excepción que acabéis de suscribiros a alguna lista o estéis en ese momento estableciendo algun tipo de relación con la entidad**.

Un efecto indeseable del robo de contraseñas, no es sólo la posibilidad acceder a tu correo, sino la emisión de spam desde tu cuenta. La implicación directa de esto es que los servicios centrales de correo son bloqueados, es decir que **por el robo de una contraseña la Universidad entera puede quedarse sin poder enviar correo**, como ya nos ha pasado.

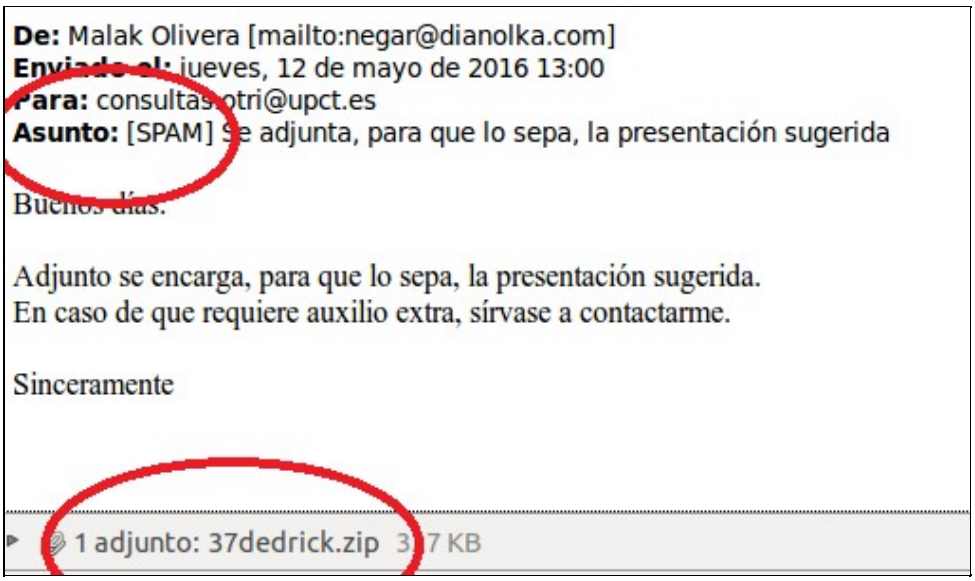
Ejemplos de correos maliciosos

Te mando un archivo adjunto

Este es de lo más típicos. Mails con las frase *mando lo que me pedistes* o *espero que te guste* inundan nuestras redes. Si miráis la imagen del siguiente correo podéis reparar en dos cosas :


```
1.- Que la dirección del remitentes es sumamente extraña
2.- Que el nombre del paquete comprimido también es extraño
y 3.- Por si fuera poco el texto resulta extraño de leer.
```

En la mayoría de los casos estos correos ya vienen con un aviso diciendo que es **SPAM**. Esta catalogación se hace desde unos servidores externos a la Universidad y les añaden esta etiqueta para avisar al usuario. No los borran directamente para evitar errores y evitar que en algunos casos se clasifiquen como spam correos legítimos.



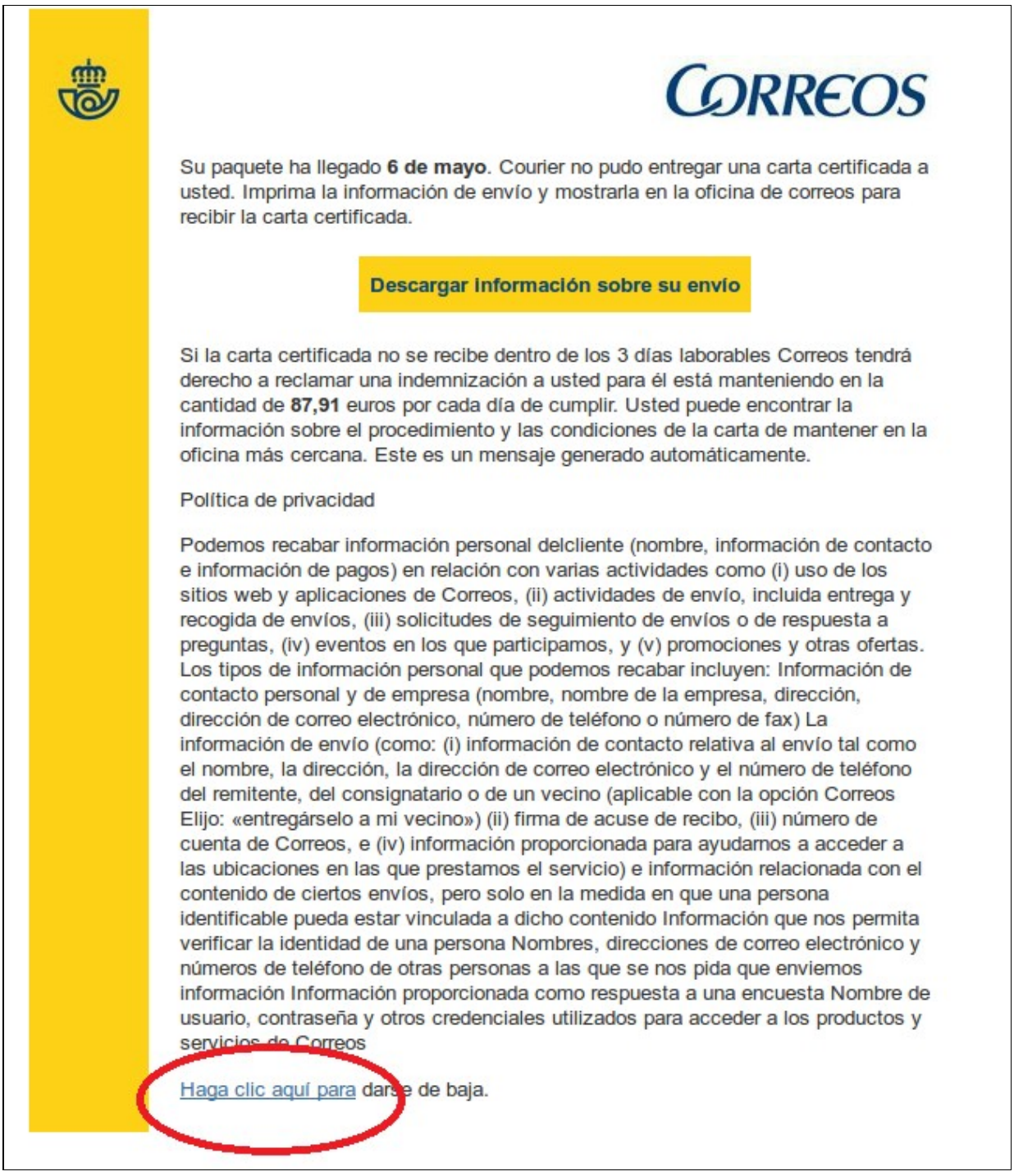
Como siempre lo mejor es borrarlos.

Envío de correos

```
Ha llegado un paquete postal a su nombre. Es necesario recogerlo en la sucursal más cercana de cor
Para ello imprima el resguardo e indique, en qué sucursal quiere recoger el paquete.
Pulse aquí para imprimir el resguardo y escoger la sucursal.
Estado del paquete: Listo para su entrega
Tipo de servicio: Express
El número de su paquete: ?????????????
Seguro: Sí
Atención! Si usted no retira el paquete durante los proximos 30 días se le cobrará una comisión de
Le pedimos recoger el paquete en menos de 30 días después de recibir este aviso.
```

Cómo podéis ver, en este correo no os piden ningún tipo de datos sino que pulséis un enlace, que seguramente os descargara un malware, virus y/o troyano. El propio Servicio de Correos ha pedido que os avisemos de que, Correos como organismo público nunca envía un correo electrónico para dar ningún aviso, sino que deja los mismos en vuestro buzón. Por favor, borrad todos los mensajes que os lleguen de este tipo.

Este tipo de correo ha ido evolucionando y ultimamente se están recibiendo correos como el de la imagen:



CORREOS

Su paquete ha llegado **6 de mayo**. Courier no pudo entregar una carta certificada a usted. Imprima la información de envío y mostrarla en la oficina de correos para recibir la carta certificada.

Descargar información sobre su envío

Si la carta certificada no se recibe dentro de los 3 días laborables Correos tendrá derecho a reclamar una indemnización a usted para él está manteniendo en la cantidad de **87,91** euros por cada día de cumplir. Usted puede encontrar la información sobre el procedimiento y las condiciones de la carta de mantener en la oficina más cercana. Este es un mensaje generado automáticamente.

Política de privacidad

Podemos recabar información personal delcliente (nombre, información de contacto e información de pagos) en relación con varias actividades como (i) uso de los sitios web y aplicaciones de Correos, (ii) actividades de envío, incluida entrega y recogida de envíos, (iii) solicitudes de seguimiento de envíos o de respuesta a preguntas, (iv) eventos en los que participamos, y (v) promociones y otras ofertas. Los tipos de información personal que podemos recabar incluyen: Información de contacto personal y de empresa (nombre, nombre de la empresa, dirección, dirección de correo electrónico, número de teléfono o número de fax) La información de envío (como: (i) información de contacto relativa al envío tal como el nombre, la dirección, la dirección de correo electrónico y el número de teléfono del remitente, del consignatario o de un vecino (aplicable con la opción Correos Elijo: «entregárselo a mi vecino») (ii) firma de acuse de recibo, (iii) número de cuenta de Correos, e (iv) información proporcionada para ayudarnos a acceder a las ubicaciones en las que prestamos el servicio) e información relacionada con el contenido de ciertos envíos, pero solo en la medida en que una persona identificable pueda estar vinculada a dicho contenido Información que nos permita verificar la identidad de una persona Nombres, direcciones de correo electrónico y números de teléfono de otras personas a las que se nos pida que enviemos información Información proporcionada como respuesta a una encuesta Nombre de usuario, contraseña y otros credenciales utilizados para acceder a los productos y servicios de Correos

Haga clic aquí para darse de baja.

La dirección a la que te dirige este mensaje si pulsas en *el enlace* ó *haga click aquí' es algo similar a esto :*

http://islamreligiapkoju.com/xPycHGZ5m1W/Sysplbjrtx7.php?id=menganito@si.upct.es

Por supuesto ni pulsar ni nada por el estilo. Correos ya ha emitido un aviso en su página web advirtiendo de estos correos.

Su correo ya está comprometido

De: Universidad Politécnica de Cartagena [1]
Enviado el: jueves, 25 de junio de 2015 10:24

```
Asunto: + Alerta administración
Estimados usuarios de la Universidad Politécnica de Cartagena,
Debido a las quejas sobre spam de correo electrónico de los usuarios del sistema de mensajería
web Universidad Politécnica de Cartagena, nuestra investigación muestra que su dirección de correo
electrónico está comprometido y utilizado para enviar spam a sistema de web de la Universidad
Politécnica de Cartagena. Por lo tanto, nuestras máquinas de la red realizará mantenimiento, deberá
hacer clic en el siguiente enlace para confirmar tu información de cuenta dentro de las próximas
48 horas o se desactivará su cuenta de correo electrónico de la Universidad Politécnica de Cartagena
de nuestra base de datos. Simplementehaga (CLICK AQUÍ) con la información completa solicitada para
completar el mantenimiento. Valoramos su negocio y gracias por utilizar nuestro servicio web.
Universidad Politécnica de Cartagena
Copyright (C) Universidad Politécnica de Cartagena: Todos los derechos reservados.
```

Se ha dectectado un virus en su correo

```
De: Universidad Politécnica de Cartagena <aglaison@pmenos.com.br>
Asunto:
Responder: webmailantivirus2020@gmail.com
Nos gustaría informarle que estamos llevando actualmente a cabo el mantenimiento programado y
la mejora de nuestro servicio de correo web y, como resultado de un virus HTK4S se detectó en
las carpetas de su cuenta, y su cuenta tiene que ser actualizado para el nuevo anti-virus F-Secure
HTK4S / Anti-Spam versión 2015 para evitar daños en sus archivos importantes. Llenar las columnas
de abajo y enviar de vuelta o de tu cuenta de correo electrónico será suspendido temporalmente
de nuestros servicios.
1 - Usuario: ...................
2 - Contraseña: .....................
3 - Confirmar Contraseña: ..................
4 - Teléfono: ............................
Si no lo hace dentro de las 24 horas inmediatamente hará que su cuenta desactivado desde nuestra b
                              © 2015 Universidad Politécnica de Cartagena
```

Tamaño del buzón de correo

El siguiente mail viene de una dirección de Gmail y amenaza con impedir el acceso al buzón de correo:

```
24, 2014 13:16
520MB 520MB tamaño electrónico de cuota del 97,9%
Se trata de advertirle de revalidar su buzón, ya que ha superado su límite de almacenamiento Como
Haga clic aquí para revalidar: http://www.psp.heliohost.org/upct.es/upct.es.htm
Administrador del Sistema Webmail
Correo electrónico Help Desk
https://correo.upct.es/horde/imp/compose.php?mailbox=INBOX
```

También hemos recibido otra versión de este mensaje suplantado al Servicio de Informática, han copiado logo y firma y como hacen normalmente piden que se clique sobre una dirección maliciosa, en este caso *http:// upct. 16mb. com*.

Carácter: Confidencial

La UPCT cuota de buzón ha superado su límite, no puede ser capaz de enviar/recibir más correos ele
Por favor, elimine cualquier elemento que no necesita de su buzón y vaciar la carpeta de elementos
La oficina de la seguridad de la información se mantendrá actualizada esta información si debe cam

Servicio de Informática (CTSI)
968-338999
http://www.upct.es/si/
© 2015 UNIVERSIDAD POLITÉCNICA DE CARTAGENA

El siguiente ejemplo, llega supuestamente desde Google. La dirección es correcta, pues Google deja crear formularios a sus usuarios, y en este caso es lo que se ha empleado para recopilar información. Google eliminó este enlace en cuanto fue advertido del caso.

Su buzón de correo electrónico ha llegado a su límite máximo de
almacenamiento de 500 MB y su cuenta será desactivada si no se
actualiza ahora. Para actualizar su cuenta de correo web, por favor
haga clic en el enlace a continuación y siga las instrucciones para
actualizar el espacio de mayor capacidad de almacenamiento.
HAGA CLIC AQUÍ:
https:// docs.google.com/spreadsheet/viewform?formkey=dFFWQ1gxNWR2dXNrWjN2QnJmWmczNmc6MQ
Su cuenta permanecerá activa después de haber confirmado con éxito su cuenta.
Copyright © 2012 # Información de Asistencia para webmasters de
administración ? TODOS LOS DERECHOS RESERVADOS ?

Otro ejemplo :

520 MB 520 MB de tamaño de correo Cuota 97,9%
Se trata de advertirle de revalidar su buzón, ya que ha superado el
límite de almacenamiento que las establecidas por el administrador, y no
vas a ser capaz de recibir nuevos correos hasta que vuelva a validarlo.
Haga clic aquí para revalidar:
http: //www.cva.heliohost.org/upct.es/upct.es.htm
Administrador del Sistema Webmail
Email Help Desk
https://correo.upct.es/horde/imp/login.php?new_lang=es_ES

En este caso no ocultan la dirección en la que piden que se clicke - en la que se le va a pedir sus datos de correo y su contraseña - sino que además ponen como referencia la dirección de webmail de la Universidad.

Confirmación de Identidad de correo

Confirmar su identidad Webmail
Su buzón ha superado uno o más límites de tamaño establecidos por el administrador. Es posible que
tamaño del buzón. Para disponer de más espacio, por favor haz click '*aquí* abajo para corregir deta
Gracias y disculpen las molestias.
Administrador De Sistema.

En este caso el enlace *aquí* corresponde a la dirección *http:// laborcounselors.com/SLG/cli/upgrade/* que nada tiene que ver, evidentemente, con la UPCT.

Suplantación de Identidad

Aprovechando el inicio de la campaña de la declaración de la renta es posible que os llegue algún correo fraudulento que simula ser de la Agencia Tributaria. Os remitimos un enlace de de la Dirección General de la Policia, dónde avisan del intento de fraude.

El correo aparece como procedente de la AEAT e informa al destinatario de una devolución y piden los datos del usuario para llevarla a cabo.

Como siempre: ninguna entidad pública pedirá por correo datos como contraseñas ó cuentas bancarias o tarjetas de crédito.

Para más información pulsad el siguiente enlace:
http://www.policia.es/org_central/judicial/udef/alertas/20110404_1.html

Virus de la policia

También incluimos un aviso de un correo de unas características un poco más especiales que circula por la red cada cierto tiempo. Se trata de un correo que se autoidentifica como de la Policía Nacional y acusa al receptor de haber cometido un delito:

```
Su dirección IP ha sido registrada en las webs ilegales con contenido pornográfico orientadas a la
pornografía infantil, zoofilia e imágenes de violencia
contra menores! [...] "
```

Con estas amenazas insta el usuario a pulsar un enlace. Este enlace instala un troyano en el ordenador.

Virus Petya

Petya es un nuevo ransomware que impide el acceso al disco duro.

Investigadores de G-Data han informado de un nuevo malware, más concretamente un ransomware, que bajo el nombre de Petya impide el acceso al disco duro y pide un rescate de más de 300 euros.Al igual que el "Virus de la policía" este tipo de malware que secuestra recursos de un sistema informático y pide un rescate por su liberación.

```
Para llevar a cabo la infección, los estafadores utilizan correos específicamente diseñados en los
alojamiento en Dropbox, que simula ser un falso currículum. A diferencia de otras ocasiones en que
vulnerabilidades  para lograr la infección del sistema, en esta ocasión los atacantes recurren al
ingeniería social. El archivo descargado en realidad es un ejecutable ("Bewerbungsmappe-gepackt.ex
instalación del troyano en el sistema.
```

Una vez instalado Petya sobrescribe el MBR (Master Boot Record) del disco duro reemplazándolo con un cargador malicioso y provoca el reinicio del ordenador. El MBR es la parte del sistema que indica al ordenador como debe arrancar el sistema operativo. Con ello Windows se reinicia con el cargador del ransomware, que muestra una pantalla que simula ser un chkdsk. Sin embargo durante este falso Chkdsk lo que realiza es el cifrado de la Master File Table (MFT).Esto es, Petya no llega a cifrar todo el disco duro como tal, lo cual llevaría demasiado tiempo, pero una vez que la MFT queda cifrada (o corrompida) el sistema no puede saber donde se alojan los archivos, por lo que quedan totalmente inaccesibles.

Tras ello, como suele ser habitual en este tipo de malware se muestra un aviso bastante alarmante. arranque de Windows se muestra una pantalla de color rojo con una calavera blanca en ASCCI. Ahora mostrar una pantalla en la que se ofrecen las instrucciones para realizar la compra de una clave q

Vídeo en el que se muestra la actuación de Petya:
https://www.youtube.com/watch?v=yfCt35RTR-U

También hay que señalar que una vez que el MBR queda modificado por Petya, también se impide el reinicio en Modo Seguro.

Acto seguido, el usuario recibe instrucciones explícitas sobre cómo hacer el pago, al igual que cualquier crypto-ransomware que esté circulando en la actualidad: una lista de demandas, un enlace a Tor Project y cómo llegar a la página de pago a través de él, y un código de descifrado personal.Las instrucciones para el pago se encuentran en una web de la red Tor,donde se informa que el afectado deberá pagar 0,90294 Bitcoins (unos 320 euros) para obtener la supuesta clave que permita recuperar la información del disco duro.

Hasta el momento todos los análisis realizados no se ha conseguido un método para recuperar la información, por lo que como siempre la mejor medida de seguridad es la precaución.

Según ha confirmado Trend Micro Dropbox fue informada de los archivos maliciosos alojados en su servicio y la compañía ya los ha eliminado. A pesar de ello, hay que tener presente que los atacantes podrán emplear cualquier otro alojamiento o medio para el envío del archivo malicioso.

Más información sobre este malware en: Petya

Virus CryptoLocker

En estos mensajes se le dice a los usuarios que tienen un paquete que no le ha sido entregado, y se le incita a hacer click en un enlace para descargar la información sobre el incidente. Del enlace nos descargamos un archivo ?informacion13219.zip? que contiene un JavaScript (ejecutable), el cual infecta nuestro equipo descargando el Ransomware desde Rusia.

El ejecutable que se descarga es un .exe que que se muestra como un icono de carpeta. Los ejecutables persisten al reiniciar el ordenador y cifran nuestros ficheros pidiendo un rescate, por lo que una vez más la mejor medicina es la prevención, y es recomendable que si recibimos este tipo de correos no entremos en sus enlaces y lo eliminemos inmediatamente.

Invitaciones a redes sociales

En este caso **aquí** corresponde a *http://invites.flipmailer.com/uns_inviter.jsp?fullname=&email=amigo1@si.upct.es&invitername=amigo&inviterid=37480733&*

Evitando el phishing

- Eliminar cualquier correo que pueda parecer sospechoso o del que no se tenga constancia del origen, sin abrirlo. Borrar cualquier correo spam o basura: no abrir sus adjuntos, ni acceder a sus enlaces.
- Evitar las cadenas de mensajes, ya que éstas son fuente de correo basura (spam) y un modo de recopilación de direcciones de correo electrónico fuentes potenciales de phishing. Para ello, lo mejor es enviar los correos con destinatarios ocultos.
- Tener instalado en el ordenador un antivirus actualizado, además de contar con las últimas versiones del software de los programas del ordenador.
- No picar en los enlaces incluidos en correos supuestamente fraudulentos o dudosos, ya que con esto se puede derivar a las hipotéticas páginas fraudulentas. Lo más seguro es teclear la dirección directamente en la barra de direcciones del ordenador.
- Recuerde que ni lo bancos, ni los organismos oficiales le van pedir nunca información de usuario, claves y datos personales a través de un correo electrónico.
- Antes de introducir datos personales en una determinada página Web, asegurarse que se trata de un servidor seguro: la dirección de la página empieza por **https** precedida de un candado de color verde en la barra de direcciones.

- Si se ha recibido alguno de estos correos o si se es víctima de un engaño de este tipo, no dude en comunicárnoslo inmediatamete si se trata de datos de usuario de la UPCT, o a la entidad a la que se le ha suplantado la identidad. También es recomendable denunciarlo a la Policía o a la Guardia Civil.

Para más información, puede hacer clic en los siguientes enlaces:
http://www.policia.es/consejos/consejos.html http://www.guardiacivil.es/es/servicios/consejos/index.html