Nota de prensa

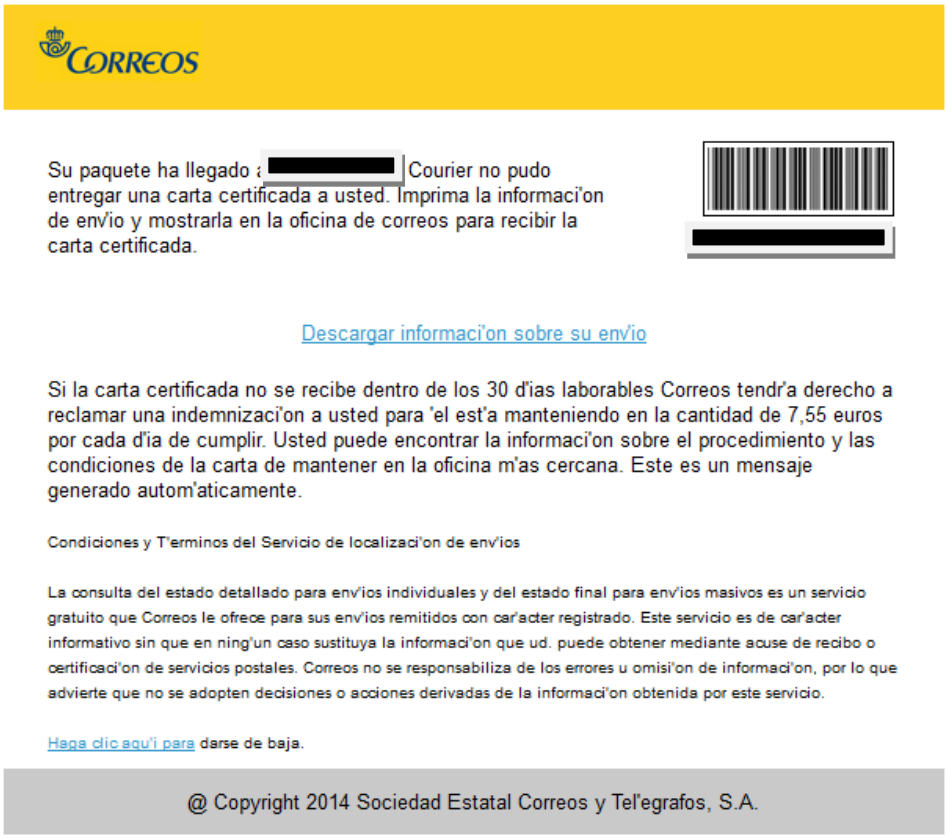
La Guardia Civil identifica el modo de infección del “virus” que encripta archivos.

- **El modo de infección procede de un phishing que suplanta la identidad de la empresa Correos España con una supuesta “carta certificada” con el objeto de engañar a los usuarios.**

Se ha detectado desde finales del año pasado y del presente una nueva campaña de phishing que suplanta la identidad **de la empresa Correos España** con una supuesta “carta certificada” con el objeto de engañar a los usuarios mediante ingeniería social. Se ha observado que dicho envió de correos electrónicos puede coincidir con la fecha de nacimiento del destinatario, hecho este que hace que abran dicho email pensando que puede ser una felicitación o regalo.

El “virus” se hace pasar por un aviso de correos, y al pulsar sobre el enlace, se descarga un fichero **.zip** llamado **carta_certificada**. Si se descomprime y ejecuta el archivo **.exe**, con el mismo nombre, se ejecuta e instala el citado “virus”.

Nota de prensa



CORREOS

Su paquete ha llegado [redacted] Courier no pudo entregar una carta certificada a usted. Imprima la informaci'on de env'io y mostrarla en la oficina de correos para recibir la carta certificada.

[redacted]

Descargar informaci'on sobre su env'io

Si la carta certificada no se recibe dentro de los 30 d'ias laborables Correos tendr'a derecho a reclamar una indemnizaci'on a usted para 'el est'a manteniendo en la cantidad de 7,55 euros por cada d'ia de cumplir. Usted puede encontrar la informaci'on sobre el procedimiento y las condiciones de la carta de mantener en la oficina m'as cercana. Este es un mensaje generado autom'aticamente.

Condiciones y T'erminos del Servicio de localizaci'on de env'ios

La consulta del estado detallado para env'ios individuales y del estado final para env'ios masivos es un servicio gratuito que Correos le ofrece para sus env'ios remitidos con car'acter registrado. Este servicio es de car'acter informativo sin que en ning'un caso sustituya la informaci'on que ud. puede obtener mediante acuse de recibo o certificaci'on de servicios postales. Correos no se responsabiliza de los errores u omisi'on de informaci'on, por lo que advierte que no se adopten decisiones o acciones derivadas de la informaci'on obtenida por este servicio.

Haga clic aqu'i para darse de baja.

@ Copyright 2014 Sociedad Estatal Correos y Tel'egrafos, S.A.

Si nos fijamos bien en la dirección del remitente, el “cuerpo” del correo, y en las extensiones del archivo adjunto, se observan indicios que puedan ayudarnos a sospechar de su procedencia (textos en inglés mal traducidos, direcciones erróneas, etc) en el caso concreto que nos ocupa, junto a la traducción defectuosa se ha observado que en vez de poner en el cuerpo del correo la palabra “**España**”, aparece “**Espana**” no coincidiendo con el organismo oficial.

Tras lo descrito, todos los datos del disco duro, quedan encriptados, incluidas unidades de red o discos duros externos conectados por USB, procediendo a cifrar los archivos con la extensión **.encrypted.**

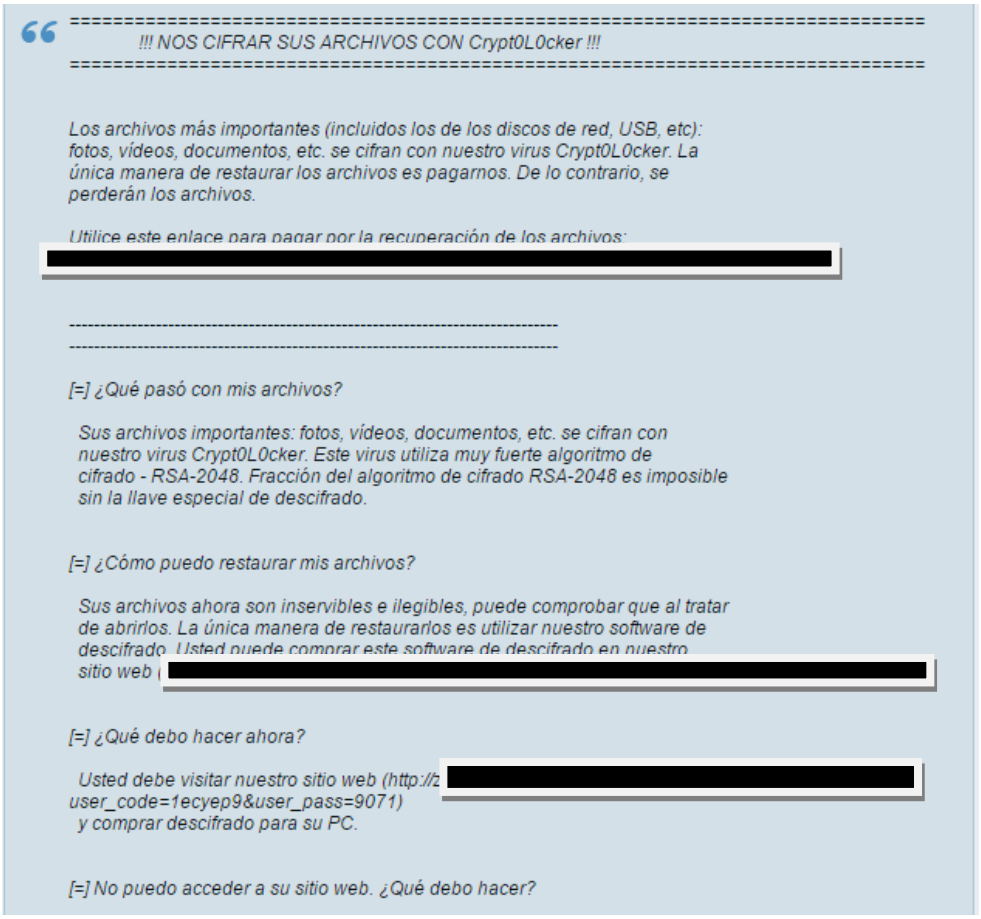
Los autores del hecho o “secuestradores” permiten que se desencripte un solo fichero de forma gratuita y el resto pagando con BitCoins (Bitcoin es una red consensuada que permite un nuevo sistema de pago criptográfico completamente digital, dificultando la identidad de los criminales).

Nota de prensa

Algunas variantes del “virus” además de cifrar los ficheros del equipo infectado, roban la libreta de direcciones para lograr nuevas víctimas a quien enviar estos mensajes maliciosos, llegando a falsificar la dirección del remitente, siendo probable que la dirección que se muestra en el correo sea la de uno de nuestros contactos.

En cada carpeta afectada del pc, se genera un documento **.txt** y otro **.html** con la siguiente “solución” con enlaces a través de la red tor.

Contenido del fichero: **INSTRUCCIONES_DESCIFRADO.txt**



```
==========================================================================
        !!! NOS CIFRAR SUS ARCHIVOS CON Crypt0L0cker !!!
==========================================================================

Los archivos más importantes (incluidos los de los discos de red, USB, etc):
fotos, vídeos, documentos, etc. se cifran con nuestro virus Crypt0L0cker. La
única manera de restaurar los archivos es pagarnos. De lo contrario, se
perderán los archivos.

Utilice este enlace para pagar por la recuperación de los archivos:
[redacted]

--------------------------------------------------------------------------
--------------------------------------------------------------------------

[=] ¿Qué pasó con mis archivos?

Sus archivos importantes: fotos, vídeos, documentos, etc. se cifran con
nuestro virus Crypt0L0cker. Este virus utiliza muy fuerte algoritmo de
cifrado - RSA-2048. Fracción del algoritmo de cifrado RSA-2048 es imposible
sin la llave especial de descifrado.

[=] ¿Cómo puedo restaurar mis archivos?

Sus archivos ahora son inservibles e ilegibles, puede comprobar que al tratar
de abrirlos. La única manera de restaurarlos es utilizar nuestro software de
descifrado. Usted puede comprar este software de descifrado en nuestro
sitio web [redacted]

[=] ¿Qué debo hacer ahora?

Usted debe visitar nuestro sitio web (http://z[redacted]
user_code=1ecyep9&user_pass=9071)
y comprar descifrado para su PC.

[=] No puedo acceder a su sitio web. ¿Qué debo hacer?
```

Nota de prensa

Nuestro sitio web debe ser accesible desde uno de estos enlaces:
http://zoqowm4kzz4cvvvl.torlocator.org/pi6nf5.php?user_code=1ecyep9&user_pass=9071
http://zoqowm4kzz4cvvvl.torminator.org/pi6nf5.php?user_code=1ecyep9&user_pass=9071
http://zoqowm4kzz4cvvvl.tor2web.blutmagie.de/pi6nf5.php?user_code=1ecyep9&user_pass=9071

http://zoqowm4kzz4cvvvl.onion/pi6nf5.php?user_code=1ecyep9&user_pass=9071 (utilizando el navegador TOR)

Si por alguna razón estas direcciones no están disponibles, por favor siga los pasos:
1. *Descargue e instale TOR-navegador:*
   http://www.torproject.org/projects/torbrowser.html.en
2. *Después de una instalación exitosa, ejecutar el navegador y esperar a que la inicialización.*
3. *Escriba en la barra de direcciones:*
   http://zoqowm4kzz4cvvvl.onion/pi6nf5.php?user_code=1ecyep9&user_pass=9071
4. *El acceso a nuestro sitio web.*

También puede ponerse en contacto con nosotros a través de correo electrónico: [redacted]

Credenciales de inicio de sesión:
URL: http://zoqowm4kzz4cvvvl.torlocator.org/pi6nf5.php
User-Code: 1ecyep9
User-Pass: 9071

==========

El autor del hecho también nos informa de los pasos a seguir para el descifrado como se observa en la siguiente imagen:

Algunos de los dominios FALSOS y REMITENTES que la Unidad investigadora ha conseguido conocer son:

correos-es.com
correos-espana.biz
correos-espana.com

GUZMÁN EL BUENO, 110
28071 - MADRID
TEL: 91 514 60 10
FAX: 91 514 60 14

Nota de prensa

correosespana.com
correos-espana.net
correos-espana.org
e-correos24.com
es-correos.com
icorreos24.net
icorreos24.org
mycorreos24.net
mycorreos.com
ptt-esube.com
ptt-gonderi.biz
ptt-gonderi.net
sda2cliente.com
sda2cliente.org
sdacourier24.info
sda-courier.biz
sda-courier.info
sdacourier.net
sdacourier.org
sda-poste.com
sda-poste.info
sdaposte.info
sda-poste.net
sdaposte.net
sda-poste.org
sdaweb24.com
sdaweb24.net
supportpiece.com

Desde el Equipo de Policía Judicial de la Guardia Civil de Costa Teguise, se recomienda que se extremen las precauciones al navegar por Internet, especialmente en correos electrónicos no solicitados y/o de remitente desconocido y, en particular, disponer de copias de seguridad actualizadas y alojadas en una unidad de disco no conectada a la red o servidor o en discos de solo lectura (Blue-Ray, DVD…), así como no descargar ni ejecutar archivos adjuntos de los que se desconozca el origen o cuyo texto no esté escrito en un castellano correcto.

Asimismo, dicha Unidad recomienda denunciar los hechos con el objeto de disponer de la mayor información posible de cada uno de los ilícitos así como a la hora de solicitar apoyo a otras Autoridades

policiales y judiciales de terceros países a facilitar la identificación de los posibles autores.

Nota de prensa