APTN COFENAT
Asociación de Profesionales de las Terapias Naturales

APTN_COFENAT INFORMA: VIRUS INFORMÁTICOS

30 de abril de 2015

Nº: 2249

INFORMACIÓN PARA EL ASOACIAD@

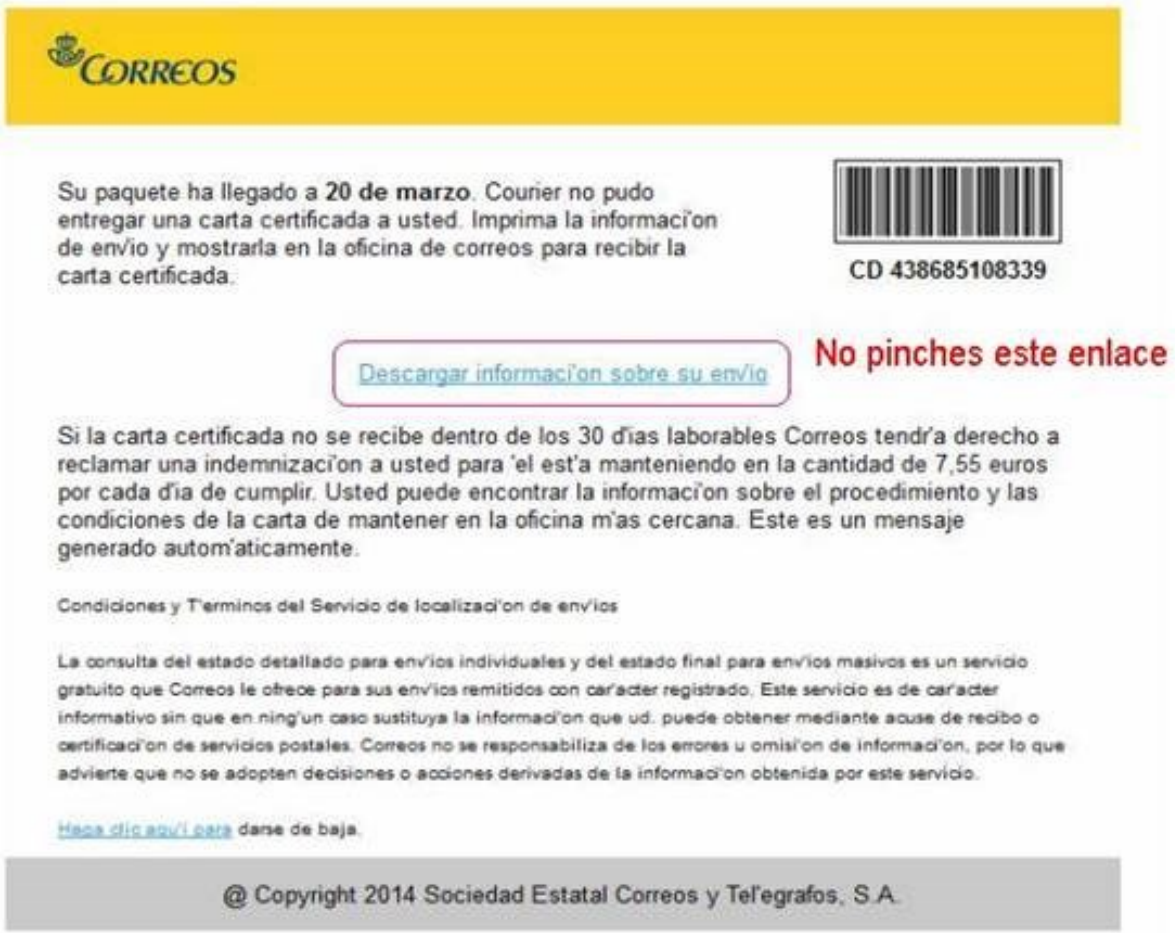
Cryptolocker, el troyano contra el que pelean en estos momentos las empresas de seguridad informática, encripta toda la información del ordenador afectado, que solo puede recuperarse si se paga un incierto rescate a los ciberdelincuentes.

Las empresas de seguridad vascas y de todo el país están en máxima alerta contra Cryptolocker, el virus más devastador contra el que tienen que vérselas en este momento. Se trata de un troyano que llega al usuario por correo electrónico y contra el que, una vez descargado por error, inercia o ignorancia, ya nada se puede hacer, aunque las diferentes compañías trabajan para encontrar la fórmula de recuperar lo datos. Todos los archivos del ordenador, incluso de la red informática si es que está conectado a otros, quedan encriptados e inservibles. Sólo se pueden recuperar si se paga un rescate a los ciberdelincuentes, en 'bitcoins' -una moneda virtual-, aunque además de ser ilegal hay pocas garantías de conseguirlo. La Ertzaintza ha admitido que más de una decena de empresas vascas han denunciado la estafa. Las compañías de seguridad informática alertan a sus clientes y les forman para evitar que queden infectados. Pero, ¿qué se puede hacer?

La estafa se presenta en un simple correo electrónico con un enlace que resulta ser el cebo que desencadena un sinfín de desastrosas consecuencias. La primera y más nefasta es la encriptación de la información que contiene el ordenador y que puede extenderse a otros equipos conectados a la misma red. La segunda, la exigencia de los estafadores del pago de una cantidad de dinero para devolver la información perdida, con escasas garantías de conseguirlo. Y la tercera, tener que formatear el ordenador para poder volver a utilizarlo, eso sí, con el disco duro rebosante de espacio disponible porque no ha quedado nada de lo que había guardado.

En eso se traduce el peligroso email que suplanta a Correos, aunque puede mudar de piel y presentarse como cualquier otro servicio tan usual como los envío postales, certificados de la DGT o de Hacienda. Desde hace semanas la Ertzaintza, la Guardia Civil, las empresas de antivirus y las de soporte informático avisan de esta nueva estafa que está afectando a un buen número de personas y empresas. En las últimas fechas la policía vasca ha recogido en las comisarías de Bilbao, Gernika, Erandio y Vitoria once denuncias de empresas y establecimientos vascos -8 en la primera semana de abril- derivadas de esta nueva estafa.

Sigue leyendo ../..



CORREOS

Su paquete ha llegado a **20 de marzo**. 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.

CD 438685108339

Descargar informaci'on sobre su env'io

No pinches este enlace

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.

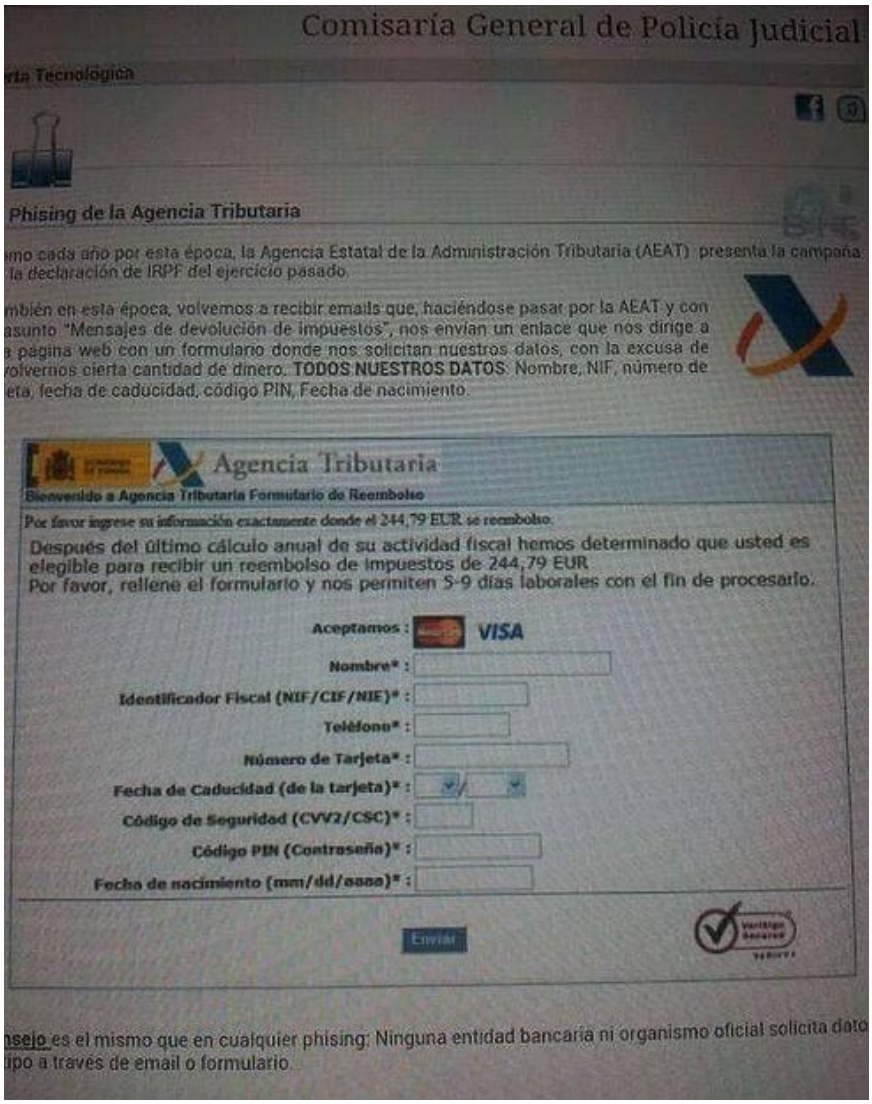
Uno de los correos electrónicos que encierran la estafa, publicado por la Guardia Civil.

A estas denuncias se añaden muchos más casos de particulares que han caído en la trampa e intentan en las redes sociales o en los foros solucionar la pérdida de sus ficheros. Ante esta oleada de casos la empresa alavesa Derten Sistemas aconseja tomar una serie de **precauciones** para no caer en las manos de los timadores. Lo primero es "desconfiar si no se espera ningún paquete de correos o si el correo proviene de una persona desconocida", aconseja **Óscar de La Fuente**, director técnico de Derten Sistemas, aunque lo más eficaz es "no abrir ningún tipo de fichero adjunto ni pinchar en links de correos que no sean de remitentes conocidos", subraya.

"No es un virus como tal, por lo que los antivirus no lo detectan", explica. Estos correos electrónicos suelen venir en otros idiomas y adjuntan un fichero comprimido, tipo 'zip', que si se abre encripta todos los ficheros que tienes en el ordenador y no los puedes volver abrir, explica De la Fuente. "Es entonces cuando te piden que si los quieres volver a abrir tienes que hacer un pago", que oscila entre "los 300 y los 3.000 euros", según ha documentado en casos ajenos a sus clientes. A este respecto, la **Ertzaintza** detalla que en algunos casos "solicitan 299 euros en bitcoins -moneda virtual de pago en internet- para recuperar los archivos informáticos dañados.

Sigue leyendo ../..

Otras modalidades



Una segunda modalidad es recibir un correo con un enlace para hacer el seguimiento de un envío, muy normal en compañías de transportes y también en Correos. Sin embargo, al pinchar en el enlace que envían los ciberdelincuentes no hay ningún seguimiento y "se ejecuta un programa que te encripta los ficheros", explica Óscar de La Fuente, quien advierte de que "casi seguro que alguno sacará algo nuevo ahora que ha empezado la campaña de la Renta". De hecho, este miércoles la Guardia Civil ha alertado de numerosos casos de 'Phising' suplantando a la Agencia Tributaria.

¿Qué hacer si has caído en la estafa?

En el caso de que se haya 'clickado' y se haya caído en la estafa, lo primero que aconseja este experto es "desenchufar el equipo de la red corporativa" para que el troyano no actúe en otros equipos conectados y, más tarde, denunciarlo.

La solución para restablecer los ficheros dañados pasa por "recuperar la información de las copias de seguridad". Si no disponen de ellas, "los archivos encriptados se habrán perdido" para siempre, porque pagar al extorsionador, además de ser delito, "no garantiza que se restablezcan los archivos". En cuanto al equipo, no habría más solución que "formatear el ordenador" para poder volver a utilizarlo, de lo contrario, "siempre queda algo que vuelve a encriptar la información", asegura el director técnico de Derten Sistemas.

Sigue leyendo ../..

¿A quién afecta?

Cualquiera que tenga correo electrónico y lo utilice puede ser víctima. "Desde empresas de 5 trabajadores a grandes compañías con miles de empleados"

Cualquier persona que tenga un correo electrónico y lo utilice puede ser víctima de esta estafa. Derten Sistemas asegura que "en los últimos dos meses todas las semanas atienden a algún cliente" afectado por este troyano "desde empresas de cinco trabajadores a grandes compañías con miles de empleados y con sofisticados sistemas de seguridad". Aunque han conseguido recuperar la información gracias a las copias de seguridad, apuntan que la solución es "mejorar las prácticas de configuración y que los usuarios estén bien informados para que no abran este tipo de archivos". Por ello, esta empresa realiza seminarios online para que sus clientes conozcan de primera mano la problemática y como abordarla. Además, sugiere implantar "soluciones que detectan que el archivo en cuestión es un documento 'raro' y lo ponen en cuarentena hasta saber si es bueno o malo"

Más información en info@aptn-cofenat.es