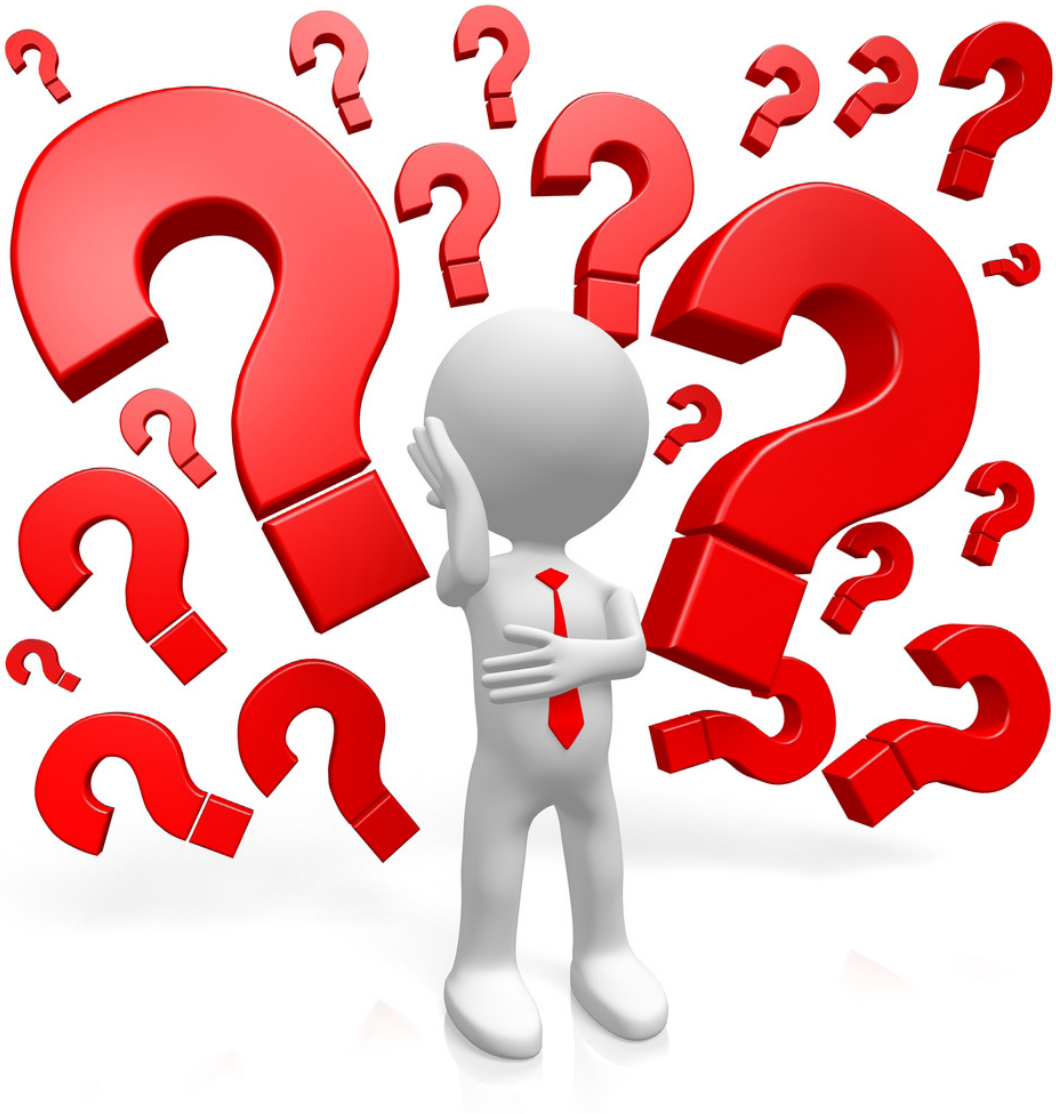
¿Estáis preparados?

Solución del Reto 1: ransomware

INSTITUTO NACIONAL DE CIBERSEGURIDAD
SPANISH NATIONAL CYBERSECURITY INSTITUTE

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL

Índice



R.1 Solución al RETO 1: ransomware

Este es el material que se ha de entregar al equipo cuando hayan debatido sobre el incidente.

1.1 ¿Qué puedes hacer?

- Llamar al soporte informático para que os ayude. El soporte informático traerá herramientas para comprobar y desinfectar los ordenadores.
- Desenganchar todos los ordenadores afectados del router para evitar que la infección se propague.
- Verificar que los demás ordenadores no están infectados.
- Cambiar todas las contraseñas, incluidas las de administración de la página web y la de la wifi, por precaución.
- Ponerse en contacto con la policía y con Incibe para ver si es algo que hubiera pasado a más gente. Es posible que conozcan el remedio, aunque llevará tiempo descifrar todos los ordenadores.
- Recuperar el correo con el adjunto malicioso accediendo desde otro ordenador. Nuestro soporte informático podrá hacer una copia cifrada para enviárselo a la policía junto con la denuncia.
- El soporte informático clonará los discos duros de los ordenadores infectados, con un procedimiento que permita conservarlos como evidencias por si hay que denunciar.
- Sacar los discos infectados para desinfectarlos y ver si se puede recuperar la información.
- Localizar las últimas copias de backup que se hayan hecho.
- Restaurar las copias de backup en discos nuevos y volver a trabajar.

1.2 ¿Qué no debes hacer?

- Ocultar que ha ocurrido algo sospechoso o que he cometido un error para que no se note y no me echen las culpas.
- Intentar resolverlo yo sólo, sin buscar ayuda. Soy un «manitas».
- Pagar el rescate para resolver el problema rápidamente.
- Seguir las instrucciones del ciberdelincuente, a ver si así se arregla todo y nadie se entera.
- Pasarle un antivirus gratuito, cambiar el disco y tirar el viejo, a ver si así puedo pasar desapercibido.
- Echarle la culpa a otro a ver si cuela.

1.3 Lecciones aprendidas: ¿cómo podrías evitarlo?

- Es importante estar preparado por si ocurre un incidente, es decir tener un procedimiento de gestión de incidencias que todo el mundo conozca para saber cómo actuar.
- Las copias de seguridad nos han salvado. Hay que hacerlas regularmente, conservarlas en un lugar externo y separado (no conectado) y probar que funcionan y sabemos recuperarlas.
- Tenemos que tener a mano la lista de contactos de apoyo y de denuncia para estos casos.
- Debemos analizar bien nuestros riesgos pues está claro que esto puede ocurrir pero no debe volver a pasar, tenemos que tomar medidas (cambiaremos de antimalware y revisaremos los procedimientos de correo electrónico).
- Informar a todo el personal de cómo actuar ante este tipo de incidentes, al fin y al cabo el comercial no lo hizo del todo mal, podría haber sido peor si no dice nada.
- Planificar sesiones de concienciación para identificar este tipo de correos y no dejarnos engañar.

GOBIERNO DE ESPAÑA
MINISTERIO DE ENERGÍA, TURISMO Y AGENDA DIGITAL

10 incibe_
2006-2016
TRABAJANDO POR LA CONFIANZA DIGITAL