

¿QUÉ TAL CLARICE...? ¿YA HAN DEJADO DE SECUESTRAR LOS FICHEROS?



Proyecto P-
45 "Audaz"



Buenas a todos ciber-navegantes. En esta entrega me gustaría hablaros de un problema de seguridad **muy serio** que está causando **estragos** a nivel mundial, y que en buena medida está en nuestra mano contener: **El ransomware**



Mirad, el *ransomware* es ese desgraciadamente famoso tipo de *malware* que, cuando se ejecuta en una máquina, **cifra nuestros archivos importantes y nos pide un rescate monetario** a cambio de poder volver a usarlos (y, muchas veces, no publicarlos...).

🔍 "Ransom" traducido al Español significa "rescate", literalmente...

¿Por qué es tan peligroso?

Esto, que inicialmente puede parecer una molestia importante para cualquier persona, alcanza niveles catastróficos cuando lo que se infecta es una empresa o institución. **¿Y eso por qué?** Pues porque este tipo de *malware* **no se limita a infectar una máquina solamente**, sino que una vez que entra en una, busca todas las que pueda que estén a su alcance de una forma u otra para hacer lo propio en ellas.

🔍 Es decir: se propaga y expande todo lo posible, cifrando todo lo que encuentre a su paso 😞

Voy a ponerte **un ejemplo**: Imagínate que tu hijo **se descarga un juego pirata** que viene "de regalo" con un *ransomware* (**caso MUY típico**). Arranca el juego y entonces el *ransomware* que tiene hace su trabajo y cifra todos los archivos de su PC. Pero, debido a eso, **¡tu ordenador también estará en peligro!** Tu hijo y tú es muy probable que compartáis la misma red, ya que tenéis acceso a Internet a través del mismo *router*, el que te da tu compañía.

🔍 **Sí, lo más típico es que seáis "vecinos de red" y el ransomware pueda "picar a tu puerta"...y, según lo que hagas, lo que esté funcionando en tu equipo o las actualizaciones que tengas...entrar 😞**

¿Cómo suele atacar?

Ahora imagínate que **eso mismo pasa en una oficina**: hay 500 ordenadores y, en 1 de ellos, un empleado abre un correo de *phishing* con un documento, estilo a los que ya comentamos en semanas pasadas.

 **No todo son imprudencias ¿eh? La mayoría son engaños muy bien orquestados. Por ejemplo, en ese correo al empleado le pueden contar que ha llegado una factura impagada urgente, y que tiene que proceder a su pago inmediatamente para no bloquear el material que su empresa necesita para trabajar. Todo con el nombre real de su jefe, de su empresa, del proveedor...;nunca sabes qué información pueden encontrar por redes sociales!**

Así que el empleado “pica” y **descarga el documento adjunto**, lo abre en su PC, y el documento le dice que para poder leer lo que pone tiene que “**Habilitar contenido**” usando todo tipo de pretextos (lo cual, dicho sea de paso, es una trampa muy común). Así que el empleado se cree el pretexto, lo hace, e inmediatamente se ejecuta el *ransomware* que venía dentro, que empieza a examinar su ordenador...y a buscar ordenadores “vecinos” vulnerables!.

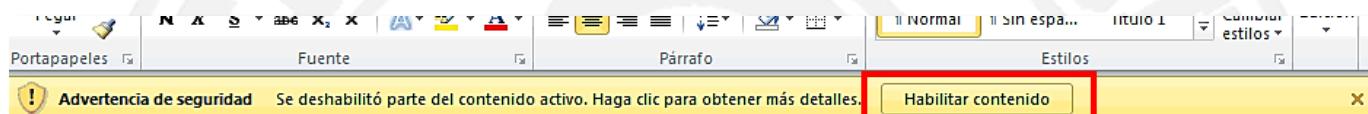


Figura 1. ¿Te sale este botón en algo que te ha llegado por correo o mensaje? No lo toques. NUNCA. JAMÁS. NO. PELIGRO. ACHTUNG.

KEEP OUT. NEIN. DANGER. PERICOLO.   

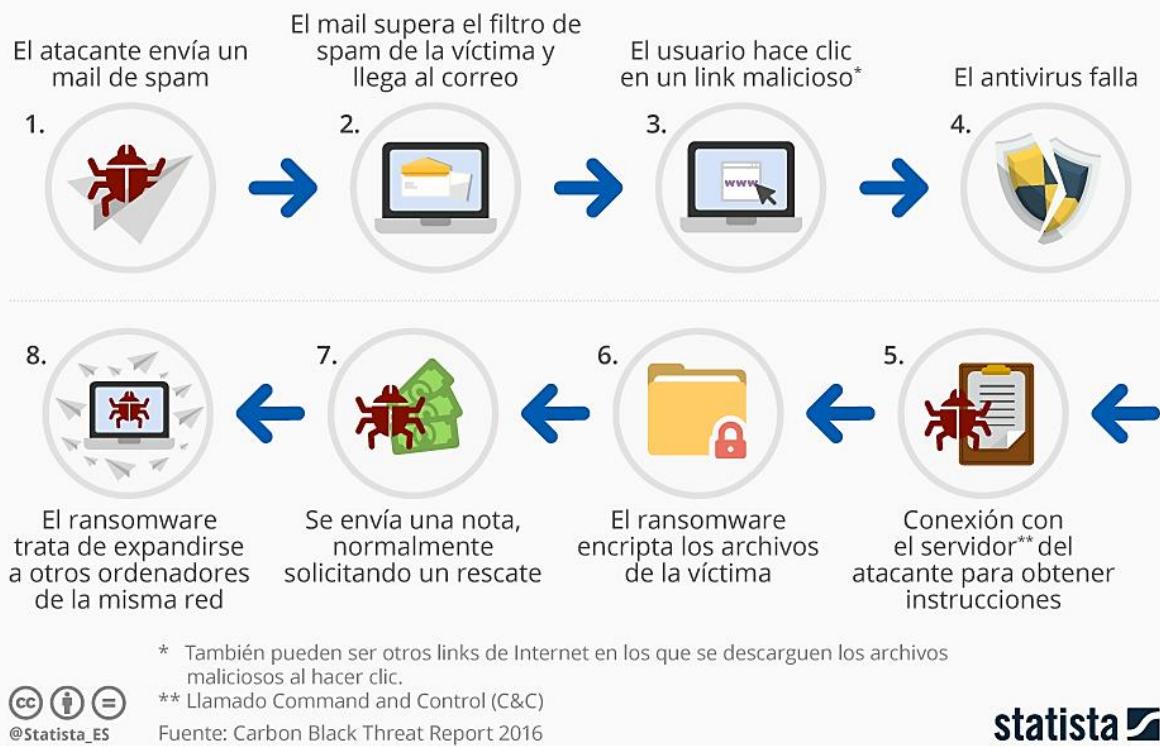
Ahora imagina que este empleado tiene, por ejemplo, **carpetas compartidas** con archivos de otros empleados en la oficina, el *ransomware* los ve, e infecta a los ficheros que hay en esas carpetas. Cuando otro empleado los abre para hacer su trabajo cotidiano, también acaba infectado. Y ese esquema de propagación, u otros similares aprovechándose de diversos fallos, se repite poco a poco hasta que al final, de una manera o de otra, **los 500 equipos de la red (todos, vamos) tienen un ransomware dentro**.

 **Hemos puesto como ejemplo un documento “con bicho”. Si te convencen para que ejecutes un programa (un adjunto con un supuesto “chiste”, u cualquier cosa que tengas que descargar y abrir) es exactamente lo mismo, pero no tienes que habilitar nada. Incluso cuando el antivirus detecta el problema, hay gente que hace caso omiso a sus advertencias y lo ejecuta 😞. Por eso a día de hoy muchos antivirus no te dejan hacer caso omiso...**

Una vez dentro...¿Cómo actúa?

¿Creéis que el ransomware cifra enseguida los archivos y da el aviso de que pagues? Pues muchas veces ¡NO!. En realidad puede estar espiando lo que hace la empresa y filtrando archivos que le manda a quién lo creo durante mucho tiempo.

¿Cómo funciona un ransomware?



statista

Figura 2. Típica secuencia de funcionamiento de un ransomware. Fuente: <https://es.statista.com/grafico/9376/como-funciona-un-ransomware>

Y como ves en la imagen anterior, al final de todo, cuando el delincuente decide que ya no puede sacar más partido, es entonces cuando ese aviso de “págame” (tienes un ejemplo de uno real en la figura siguiente) aparece.

🔍 En otras palabras: cuando ves el aviso ya es demasiado tarde 😞



Figura 3. Un aviso de pago típico. Fuente: <https://www.incibe.es/empresas/te-ayudamos/servicio-antiransomware>

¿Qué consecuencias tiene?

La consecuencia típica de un *ransomware* es que en toda la empresa **nadie puede trabajar**, porque los delincuentes que lo crean saben lo que es importante, y te bloquean el acceso a eso. El **aviso de pago** tiene una serie de características:

- **Se mete prisa** para precipitar la decisión y limitar la capacidad de respuesta con intimidación: Te vamos a destruir la información, te vamos a subir el precio, vamos a publicar tus archivos...
- **El medio de pago es muy difícilmente trazable**: Normalmente criptomonedas
- **Se ofrece prueba de que pueden descifrar** lo que te han robado
- **Se informa de que se han borrado todas las copias de seguridad** para que no puedas recuperar la información de otras formas (lo cual la mayor parte de veces es cierto, si la empresa no está preparada adecuadamente para un ataque así)
- **A veces se quedan “vigilando”** para ver qué hace la empresa, porque dejan elementos que espían las comunicaciones si se hacen con los equipos infectados. Esto puede dar lugar a respuestas aún peores si lo que la víctima hace no les gusta.

Por ello, a la empresa no le queda más remedio que parar la actividad (**perdiendo dinero y reputación** a cada segundo), y **llamar a un equipo de respuesta a incidentes profesional** y con experiencia que pueda buscar la mejor forma de deshacer el tremendo lío en el que se han metido. Y, si eres un particular, **ponte en contacto con el 017 del INCIBE**.

💡 *Esto no es broma ni exageración. Gran cantidad de grupos criminales de ransomware funcionan como empresas con mucha experiencia y saben perfectamente o que hacen. No eres más listo que ellos y, en todo caso, no quieras comprobar si lo eres porque hay mucho en juego. Déjale el trabajo a un profesional que te asesore.*

Y ahí está el problema, en **parar la actividad para hacer que el ransomware no se siga propagando**. Esto es muy grave en cualquier negocio, pero ahora imagínate estas situaciones:

- Qué ocurre **en un hospital** (como pasó en el HUCA de Asturias y en muchos otros): **podría morir gente** por ser incapaces de acceder a sus historias si se dan casos urgentes. Retrasar operaciones urgentes, sesiones de terapia contra el cáncer porque las máquinas son inoperables...
- Qué ocurre **con un servicio público**: Por ejemplo, esto pasó en el SEPE al inicio de la pandemia, y entonces hubo gente que **no pudo cobrar su subsidio de desempleo a tiempo** porque sus datos estaban inaccesibles, pasando enormes dificultades económicas. Ahora imagínate que consiguen atacar al servicio de agua potable, luz, Internet...

¿Entiendes ahora por qué hay tanta preocupación por este tipo de ataques?

💡 *No, no estoy siendo catastrofista. Si un grupo de ransomware consigue paralizar un servicio público puede tener unas consecuencias gravísimas para un sector de la población que puede ser amplio. Un auténtico acto de guerra...*

¿Por qué has hecho un boletín solo para el ransomware?

Estos son solo dos ejemplos de lo grave que puede llegar a ser el *ransomware*; Pero hay muchos otros más, solo tenéis que buscar en las noticias....Y os cuento esta historia porque sí que hay una cosa que podéis hacer para contribuir a que el *ransomware* se propague: **formaros y no hacer lo que hizo el empleado**. No os dejéis engañar por correos que os meten prisa y tienen adjuntos o enlaces, porque como podéis, ver la que podéis liar puede ser enorme.

Si quieres saber qué más puedes hacer, la siguiente infografía del INCIBE te lo explica 😊



Figura 4. Información general de como actuar ante un ransomware. Fuente: INCIBE

Y aunque todas las semanas os digo que la seguridad se consigue entre todos, y que **no se te olvide contar este estafa a tus amigos, conocidos o familiares**, esta vez os lo voy a pedir especialmente, porque realmente evitar que entre un *ransomware* en tu empresa puede incluso suponer incluso la diferencia entre que la empresa cierre o siga abierta. Así que, más que nunca ¡Que corra la voz!

¡Y esto es todo! Muchas gracias y... ¡nos vemos en la próxima entrega!

Y recuerda amigo/a, descargar y abrir / ejecutar algo en tu equipo es un gran poder... ¡que conlleva una gran responsabilidad!



¿Quieres escuchar como hablo de esta estafa en menos de 5 minutos?



- [Escúchalo en IVOOX](#)
- [Escúchalo en Amazon Podcast](#)

¿Quieres leer alguna noticia/artículo relacionado?



- [Cómo actuar en caso de un ataque de ransomware \(INCIBE\)](#)
- [Cazando ransomware \(Kit de Explorador INCIBE\)](#)
- [Así fue el ciberataque por «ransomware» que puso en jaque al servicio de salud de Asturias \(20/12/2021\):](#)
- [El ciberataque desde una dirección rusa obliga al Ayuntamiento de Gijón a revisar todos sus equipos \(26/04/2022\):](#)

Este documento usa material generado con IA²

¹ Audio emitido en "Más de Uno". 95.2 Onda Cero Oviedo (<https://www.ondacero.es/emisoras/asturias/oviedo/directo/>) el 07/11/2022

² Las imágenes del texto del documento han sido generadas con la IA Bing Chat