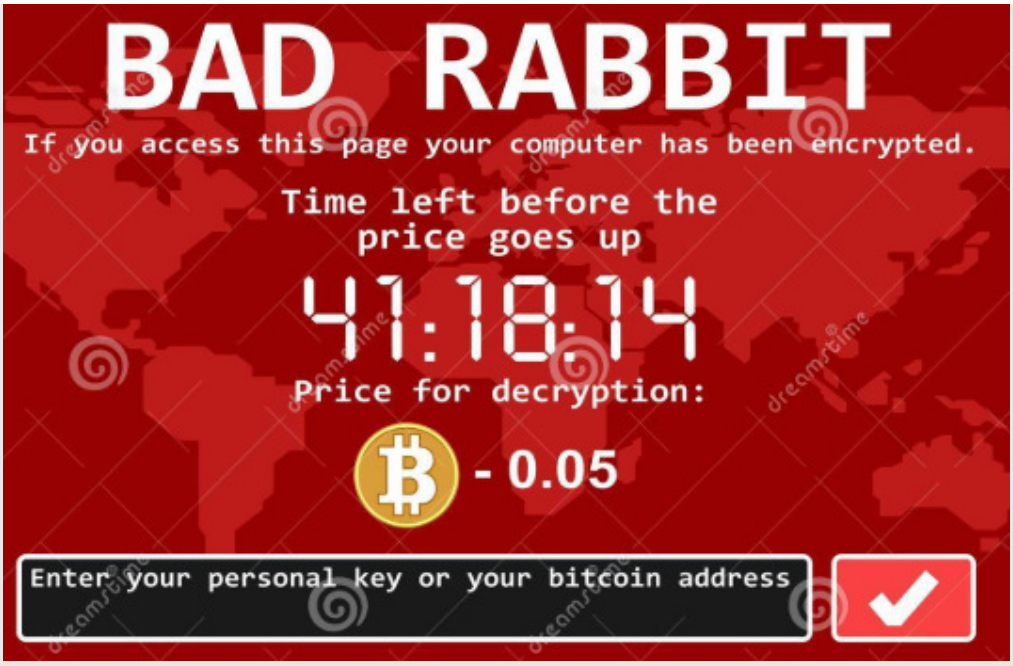
Tratamiento Ransomware

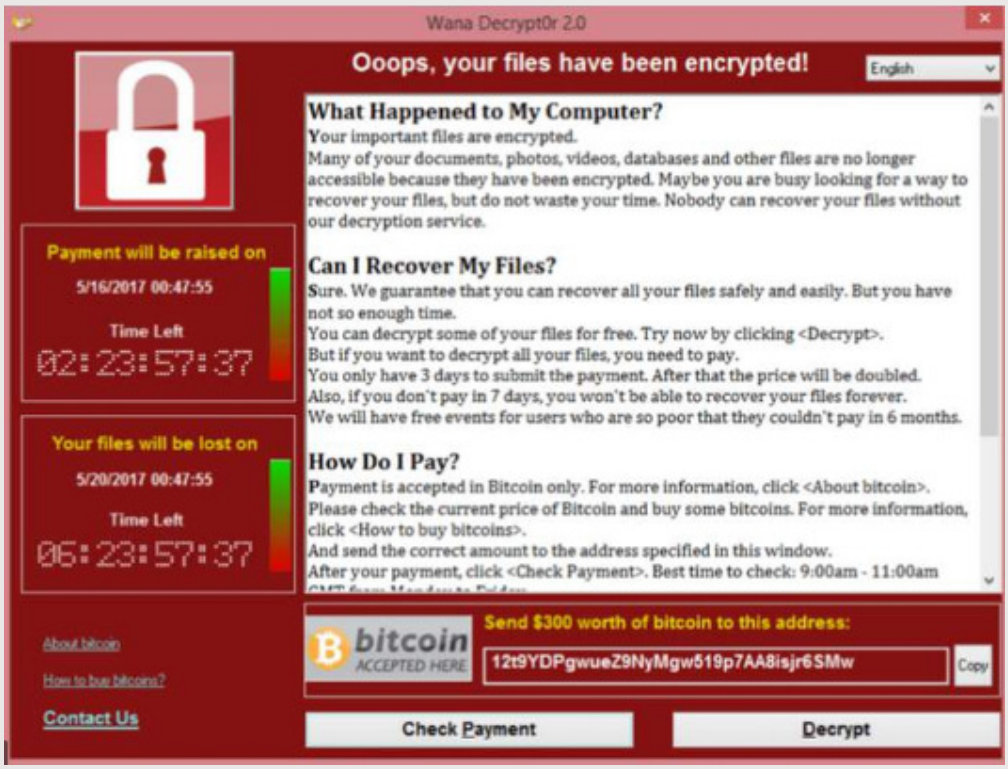
Un **ransomware** es un malware que ha estado muy presente en los últimos tiempos y representa un porcentaje que viene en constante crecimiento comparado con el resto de las amenazas informáticas en todo el mundo.

Como sabemos, otorga al atacante la posibilidad de inutilizar parcial o totalmente la PC, ocasionando la imposibilidad de abrir ciertos archivos, acceder a discos duros completos o utilizar servicios con normalidad. Su objetivo es secuestrar nuestro equipo y a cambio pedir dinero para liberarlo.

A continuación se copian algunas muestras de infecciones de distintos tipos de ransomwares.

"Su página web está bloqueada.Transfiera 1,4 BitCoin a la dirección WWWWWWWh8Q6d2j1B4XXXXXXXXXT4vTDbSM9 para desbloquearla."





Posterior a la infección se suele pedir el rescate o liberación de las llaves de desencriptado, mediante un pago que suele ser en **bitcoins.**

¿Por qué piden el rescate en bitcoins?

Los bitcoins son monedas virtuales o criptomonedas, que permiten el pago anónimo entre particulares. Este anonimato se incrementa accediendo al servicio de bitcoins desde la red anónima TOR y permite realizar una especie de lavado de la criptomoneda que dificulta que se pueda seguir el

rastro de las transacciones. Esto facilita que los cibercriminales puedan extorsionar a sus víctimas sin que la policía pueda seguirles la pista.

A continuación**, algunos consejos** para evitar ser una víctima de este tipo de malware:

Primero debemos de saber que **no todos los ransomware son iguales**. Algunos cifran archivos y no podemos abrirlos. Otros por su parte nos bloquean la pantalla, por ejemplo. Lo cierto es que cada día hay nuevas víctimas y se hacen más fuertes los atacantes.

Pero, **¿por qué cada vez afecta a más gente?** La razón es que resulta muy sencillo infectarse. Un ransomware se puede camuflar como un archivo/link inofensivo en un email o dentro de un programa que actúa como señuelo. Éste suele ser algo llamativo para la víctima, que visualmente no presenta ningún peligro. Esto provoca que lo instale y quede infectado el equipo.

Seguro que todos alguna vez hemos navegado y de repente nos ha saltado una **ventana emergente** que nos informa de que hemos ganado un premio o el típico caso que al acceder a un sitio no confiable nos sale una alerta diciendo que nuestro equipo está en riesgo y que debemos actualizar o instalar cierto programa. Esta es una de las principales entradas de ransomware y donde los usuarios pueden caer en la trampa con más facilidad.

Sentido común

Uno de los puntos clave, como podemos imaginar, es **utilizar el sentido común**. No descargar ningún tipo de archivo de dudosa procedencia. Lo mismo ocurre con posibles páginas que nos llegan en ventanas emergentes. No navegar por ellas a no ser que sepamos realmente qué son.

¿Cómo podemos protegernos o evitar ser una víctima de ransomware?

Aquí van algunas pautas a seguir.

- Lo primero es **mantener nuestro equipo actualizado** y con un buen software de seguridad.
- Otra solución es contar con un **firewall** o cortafuegos. Pero no únicamente tenerlo, sino que esté correctamente configurado y funcional. Esto permite que solamente las aplicaciones seguras y que nosotros queremos, tengan acceso.
- También es muy conveniente contar con una buena herramienta de **filtrado de spam** en nuestro servidor. Como sabemos, en muchas ocasiones un ransomware utiliza el spam para atacar a la víctima.
- Navegar siempre **en páginas seguras**. Esto ya va más relacionado con el sentido común. No significa que únicamente naveguemos por páginas que conozcamos realmente, sino que al hacerlo por otras nuevas no hagamos click en ningún enlace sospechoso o evitar que nos lleve a una nueva ventana que nada tenga que ver con la página principal.
- Tener siempre un ojo puesto en las **extensiones de los ficheros**. Con esto nos aseguramos que abrimos archivos con extensiones conocidas. Así podemos evitar posibles ejecutables que se camuflan.

Cuidado con los correos

- No abrir **archivos adjuntos** de correos electrónicos desconocidos. Esta es una de las principales entradas de ransomware. Por tanto, cualquier correo electrónico que recibamos y no conozcamos la procedencia y no tenga nada que ver con algo relacionado con nosotros y que además tiene uno o varios archivos adjuntos, eliminarlo directamente.
- Hacer **copias de seguridad** de los archivos. Esto en sí mismo no previene de ser atacado por un ransomware, pero si tenemos hecha una copia de todos nuestros archivos, el daño será mucho menor.
- **Deshabilitar las macros** en Microsoft Office. Los delincuentes utilizan JavaScript para infectar a la víctima, pero también lo hacen a través de macros maliciosas.
- **Cuidado también con los móviles**. Evitar instalar aplicaciones desconocidas o de dudosa procedencia, siempre consultar al técnico amigo.

Nunca pagar el rescate.

- En caso de que tu equipo sea infectado con ransomware la recomendación de las principales autoridades y expertos de seguridad es no pagar el rescate. Si lo haces, **no hay garantía de que recuperes el acceso a tus datos** o tu dispositivo, ni de que restos de malware puedan permanecer en tu equipo y ser reactivados. Además, al pagar estás financiado a grupos delictivos y animando que continúen las actividades