Ramsonware. Secuestros en un mundo digital.

A lo largo de la historia los secuestros han sido una tipología de delito que siempre ha existido. Piratas, bandoleros, sicarios…. Con la llegada de Internet era una simple cuestión de tiempo que este delito, al igual que muchos otros como el acoso, dieran su salto al mundo virtual.

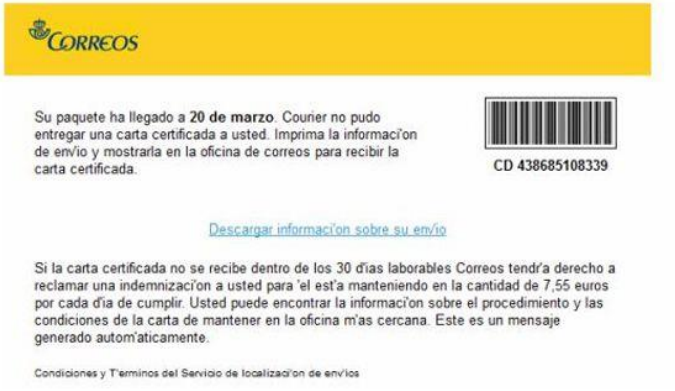
¿Cómo se ha producido ese salto? A través de una tecnología que se conoce como Malware. Se trata de una pequeña pieza de código que entra en nuestros ordenadores y una vez ahí comienza el problema. La infección se produce como con cualquier otro virus,a través de un correo electrónico (como el de la imagen inferior) con un ejecutable infectado o con un acceso a una página web comprometida o conectando un dispositivo que contenga el malware, utilizando siempre una vulnerabilidad conocida de algún programa en nuestro equipo. En este momento se transfiere a nuestro ordenador un software que realiza una serie de acciones, entre ellas la descarga e instalación de los programas que necesita para realizar su ataque. Además hay que tener en cuenta que el delito se está extendiendo a nuevos dispositivos, los teléfonos móviles son ordenadores, pero con menos prestaciones y potencia que los ordenadores tradicionales, esto hace que sean más vulnerables.

Este ataque ha evolucionado a lo largo del tiempo, inicialmente un ramsomware del tipo de "el virus de la policía" nos indicaba que habíamos cometido un delito y que debíamos pagar una multa bloqueándonos la el ordenador hasta abonar la misma. Posteriormente han evolucionado tecnológicamente incorporando al ataque el cifrado de toda la información de nuestro disco duro, y mostrando en la pantalla una imagen como la del ejemplo. En ella se nos indica que si queremos recuperar la información "secuestrada" debemos abonar un rescate. El importe varía dependiendo de si se trata de un ataque masivo en internet (puede ser desde unos 100 € o un ataque dirigido a una empresa o institución en concreto podría ascender a varios miles de euros). A cambio del rescate se nos ofrece la promesa de proporcionarnos los medios para poder recuperar nuestra información.

El pago del rescate no garantiza la recuperación de la información, el atacante puede proporcionar los medios para recuperar los datos …. o continuar con el chantaje y solicitar otras cantidades adicionales¿Qué se puede hacer en caso de infección? Depende del Ramsomware que nos haya infectado. Los más antiguos y menos evolucionados se podían eliminar por expertos en informática con programas antivirus o antiMalware. Actualmente con la incorporación del cifrado del disco duro la solución es mucho más compleja. No nos engañemos los sistemas de cifrado se han diseñado para que no puedan romperse, aunque recientemente se han analizado ramsomware cuyo algoritmo de encriptación no era robusto y era posible romperlo con el soporte de un técnico informático especialzado o un perito..

La cuestión es ¿pagar o no pagar?. Cada uno tiene que evaluar su situación, como perito he tenido conocimiento de casos en los que la infección en una empresa afectó no sólo al ordenador en el que comenzó el ataque sino a las unidades de red y servidores de datos de la red corporativa comprometiendo TODA la información corporativa, incluidas las copias de seguridad, que en el momento del ataque estaban accesibles desde el ordenador infectado. No obstante nuestra opinión es que no hay que pagar, por variios motivos.

1. El pago del rescate no garantiza la recuperación de la información, el atacante puede proporcionar los medios para recuperar los datos …. o continuar con el chantaje y solicitar otras cantidades.
2. Si se ha producido un ataque de este tipo es recomendable formatear el equipo para eliminar cualquier rastro del malware, esto implica la restauración de la copia de seguridad de los datos (si existe), con lo que el trabajo hay que hacerlo del mismo modo.



3. Se trata de un delito, si se paga se está fomentando que continúen los ataques, actualmente es un "negocio" muy rentable, no hay datos cuantificables, pero se estima que este tipo de ataques generan a los delincuentes la cantidad de 30 millones de dólares al año. Es obvio que si nadie pagara a medio plazo los ataques cesarían.

Qué se puede hacer para prevenir los ataques.

1. Mantener actualizado el sistema operativo y navegador para que los delincuentes no puedan utilizar las vulnerabilidades conocidas.
2. Desinstalar los plugins y complementos que se utilicen
3. Tener instalado, configurado y actualizado un antivirus y antimalware, no tiene que ser un servicio de pago, existen muy buenas soluciones gratuitas, pero el no tenerlo es como si dejáramos la puerta de nuestra casa abierta constantemente, ¡cualquiera puede entrar!.
4. Configurar en el ordenador cuentas de usuario sin permisos de administrador y utilizarlas para las operaciones diarias y la navegación en internet, esto dificulta la entrada del virus y protege carpetas de sistema.
5. **Disponer de copia de seguridad periódica de nuestros datos sensibles y asegurarse que la copia de seguridad no esté accesible permanentemente desde el ordenador.**
6. No conectar discos, dispositivos USB, teléfonos móviles, etc a nuestro dispositivo sin verificar que están libres de virus (se puede configurar la mayoría de antivirus para que revisen los dispositivos antes de permitir su uso)

7. No instalar software pirata, en el 80% de los casos que desde Informática y peritaje se han estudiado, el software pirata descargado de Internet incorpora malware, spyware o virus.
8. No instalar software para desbloquear nuestros dispositivos. Esta acción implica la ruptura de la seguridad de nuestro dispositivo y por supuesto implica que la puerta queda abierta para otros programas no deseados.

En definitiva, la prevención es la mejor solución, pero hay que ser conscientes que la tecnología evoluciona muy deprisa. No se puede estar seguros al 100% de evitar la infección, pero con las medidas preventivas que se han definido sí se puede realizar reducir el riesgo de la amenaza y en su caso ejecutar una recuperación de los datos perdidos.

.

Autor: Carlos Pintos Teigeiro
Informática y Peritaje
http://www.informaticayperitaje.com