Ransomware

Un Ransomware típico infecta un ordenador personal o dispositivo móvil, bloquea el funcionamiento y/o acceso a una parte o a todo el equipo apoderándose de los archivos con un cifrado fuerte y exige al usuario una **cantidad de dinero como "rescate" para liberarlos**.

Algunos consejos:

- Realizar copias de seguridad de los datos importantes como tarea de mantenimiento regular es la medida más efectiva para minimizar los daños en caso de ser infectado. La copia de seguridad debe alojarse en un medio externo distinto al del equipo para poder recuperar los archivos desde un sitio "limpio" y no tener que pagar el "rescate" exigido por estos ciberdelincuentes.
- Mantener el sistema operativo actualizado con los últimos parches de seguridad.
- Conviene instalar y mantener una solución antimalware, incluyendo un cortafuegos correctamente configurado
- Muchos de los ataques por Ransomware se distribuyen a través de campañas masivas de correo electrónico, consejos: Extremar las precauciones ante emails de remitentes no esperados, especialmente para aquellos que incluyen ficheros adjuntos.
- Aplicaciones como Privacy Manager (extensión de Chrome – mejora el control sobre la privacidad) bloquean la ejecución de todo código JavaScript sospechoso de poder dañar el equipo del usuario. Esto ayuda a minimizar las posibilidades de quedar infectado a través de la navegación web.
- Utilizar para tareas comunes un usuario común y solo dejar el administrador para cuando se vaya a hacer una serie de tareas relacionadas con la manipulación del sistema.
- Mostrar las extensiones para tipos de ficheros conocidos es una buena práctica para identificar los posibles ficheros ejecutables que quieran hacerse pasar por otro tipo de fichero.
- Utilizar herramientas que faciliten el establecimiento de políticas que impiden la ejecución de directorios comúnmente utilizados por el ransomware, como App Data, Local App Data, etc. Ejemplo: AppLocker, Cryptoprevent.
- Utilizar una herramienta específica contra este tipo de ataques (Anti Ransom), que tratará de bloquear el proceso de cifrado de un ransomware (monitorizando "honey files"). Realizará un dump de la memoria del código dañino en el momento de su ejecución, en el que con suerte hallaremos la clave de cifrado simétrico que estuviera empleándose.