



Oficina de la Fiscalía ▪ *Distrito Judicial 18*

Fiscal de Distrito George H. Brauchler ▪ Condados de Arapahoe, Douglas, Elbert & Lincoln

Advertencia al Consumidor **Consumer Advisory**

Lecciones aprendidas del ataque de Ransom-ware 'WannaCry'

Casi todos están al tanto del virus de ransom-ware que infecto a miles de computadoras a nivel mundial recientemente. El golpe, conocido como 'WannaCry' (*Quiero llorar*), paralizó computadoras y amenazó con borrar toda la información almacenada a menos de que se pagara un monto de dinero a los extorsionistas para descifrar los archivos. Varios sistemas operativos de Microsoft fueron afectados, principalmente redes que aun no habían instalado el patch de seguridad que se emitió en Marzo cuando se detectó la vulnerabilidad por primera ocasión. También resultaron afectados hospitales y organizaciones de Asia y Europa que estaban operando con el sistema Microsoft Windows XP así como otro sistema de Microsoft más antiguo al cual dejaron de dar soporte técnico en el 2014. Lo más sorprendente fue que las víctimas no habían respaldado su información en un disco externo, lo cual generó el ataque.

A pesar de que el virus de ransom-ware ha existido desde ya algún tiempo, el ataque 'WannaCry' es el más difundido a la fecha. Este ataque, que causó el cierre de hospitales y sistemas de emergencia debe servir como una advertencia así como una oportunidad para aprender una lección valiosa. Si la ponemos en práctica, nos puede aportar protección en contra de un delito del ciber-espacio que es particularmente dañino y que se sospecha ira en aumento.

- ❖ **Acostúmbrese a respaldar su información crítica almacenada en su computadora.** Es la medida precautoria más eficiente en contra de un ataque ransom-ware. Otras opciones para respaldar su información sería almacenarla en la nube o bien en un hard-drive externo.
- ❖ Actualice sus sistemas operativos por medio del fabricante. Los sistemas operativos obsoletos tienen un mayor riesgo de ser infectados a pesar de que instale firewalls y sistemas antivirus.
- ❖ Mantenga el software de seguridad actualizado. Mantenga la configuración activa de manera que el sistema se actualice en forma automatizada.
- ❖ No use software no registrado o sin licencia (pirata), ya que las actualizaciones del sistema no funcionan sobre sistemas de software sin licencia.
- ❖ Visite y abra únicamente los sitios de red y correos electrónicos de confianza. Cuando tenga alguna duda es preferible no abrirlo.
- ❖ En caso de que sufra de un ataque ransom-ware no haga el pago que le exijan. Los delincuentes no son personas de confianza y aunque haga el pago eso no le garantiza que van a des-bloquear su computadora. Contrate a un profesional para solucionar el problema y para detectar si existe algún otro virus o algún otro defecto. Por favor recuerde que aun así, es poco factible que los archivos atacados por el ransom-ware puedan recuperarse.
- ❖ Apague su computadora o desconéctela del internet cuando no la este usando.
- ❖ Sea muy cauteloso cuando utilice la conexión Wi-Fi en lugares públicos. Escoja las configuraciones que muestren que usted está en un lugar público. El hacer esto permite bloquear conexiones no seguras a puertos externos.

- ❖ Si usted no está muy familiarizado con las computadoras o los últimos avances en tecnología computacional o el vocabulario que se utiliza, quizá sea una buena idea pedirle a algún amigo de confianza o pariente que sea el administrador de su computadora.

Distrito Judicial 18
Línea telefónica de protección en contra del fraude:
720-874-8547