Ataques recientes

En los últimos días una de las noticias mas mencionadas en el mundo cibernético es de una nueva hola de ataques por un virus de tipo Ransomware (ransom viene del inglés “rescate” y ware por “software) llamado WannaCry. Recordemos que los Ransomware son programas informáticos malintencionados que restringen el acceso a partes o archivos de tu sistema operativo y que una vez infectado el sistema te llega algún tipo de mensaje indicándote una cantidad a pagar si deseas volver a hacer uso de tus archivos.

¿Qué es WannaCry y como opera dentro de mi computadora?

Como mencionamos WannaCry es un tipo de Ransomware, fue descubierto por primera vez el 12 Mayo y que en lo últimos días ha logrado infectar a un impresionante número de equipos de cómputo en más de 150 países en un corto tiempo, debido a esto es considerado por el momento como el peor ciberataque del 2017 ya que ha logrado dañar severamente a negocios que incluyen pero no se limitan a hospitales, oficinas gubernamentales y bancos.

Como habíamos mencionado,la forma en que este tipo de virus es programado hace que una vez que infecta un equipo de computo en muy poco tiempo logra encriptar todos o un gran número de archivos así como puede también encriptar parte del sistema operativo. Una vez que haya logrado bloquear el acceso a tus archivos, pronto el usuario recibirá un mensaje donde indica la cantidad que debe pagar si es que se desea recuperar los archivos encriptados.

En el caso de WannaCry, por la información que se ha compartido en la Internet por usuarios que fueron víctimas de este ataque, el software advierte que se necesitarán 300 bitcoin para permitir al usuario recuperar los archivos, si el pago se tarda mas de 3 días, el precio sube a 600 bitcoin y una vez que han transcurridos 7 días sin que se haya hecho algún pago, el virus procederá a borrar permanentemente todos los archivos encriptados.

¿Qué medidas puedo tomar para reducir el riesgo de que se infecte mi computadora?

Para lograr reducir la posibilidad de ser infectados es importante que cada empresa trabaje de la mano con su departamento de sistemas y considerar las siguientes sugerencias:

Continuamente respaldar tu información: Esto debe de ser de las tareas más comunes que debe de estar haciendo toda empresa con su información, programar recordatorios para llevar a cabo esta tarea, semanalmente seria buena práctica, aunque la importancia de la información que se genera a diario determinara si se requiere que se haga el respaldo con mayor frecuencia. Si se da el caso que tu computadora llegue a infectarse, seria muy fácil restablecer todos tus archivos, o la mayoría de ellos ,a su estado original antes de que hallan sido "secuestrados" por un programa malicioso.

Ser muy cautelosos con los corres electrónicos recibidos: Revisar en todo tiempo el remitente del mensaje, tener cuidado con cualquier correo que te invite a abrir un archivo o dar clic en un enlace que viene en el mismo mensaje. **Es importante que cada empresa establezca políticas de lectura de correos**. Si no conoces la fuente del correo eliminalo, si llega un correo de alguien y no puedes recordar la conversación con el contacto eliminarlo.

Mantener tu equipo y programas actualizados: Es de suma importancia que cada empresa planifique con su departamento de sistemas para establecer con que frecuencia se actualizarán los equipos y si conviene o no llevar acabo dichas actualizaciones. Cada caso es distinto y se debe de analizar los programas que maneja la empresa y ver como se puede minimizar los riesgos de una infección sin sacrificar o entorpecer el trabajo de la misma.

Se ha vuelto tan frecuente este tipo de ataque, ya que da un buen resultado para los ciber criminales, pues cuando un usuario se encuentra en una situación así, es muy fácil pagar por recuperar nuestros archivos importantes, pues pensar en la posibilidad de perderlos para siempre resulta el peor de los dos males.

Puedes hacernos llegar tus comentarios al siguiente correo:

boletin.tecnico@aaareynosa.org.mx