RISCCO

IT Risk & Security
Internal Audit

RANSOMWARE
CIBERSECUESTRO

Cuando el rescate se paga
por los datos digitales y no por personas

8 de Junio de 2015

CONTENIDO

1. Resumen Ejecutivo
2. ¿Qué es *Ransomware* o Cibersecuestro?
3. ¿Quiénes son las víctimas?
4. ¿Cómo nos afecta?
5. ¿Qué hacer?

© 2009 - 2015 RISCCO. Todos los derechos reservados.

1. RESUMEN EJECUTIVO

Ransomware o ***Cibersecuestro*** es una amenaza cibernética que encripta (cifra) y le impide tener acceso a documentos y bases de datos de su computador o dispositivo móvil. Para recobrar el acceso, usted debe pagar entre US$300 y US$6,000 a bandas de cibercriminales, ya que, de lo contrario, no podrá tener acceso a tales documentos y bases de datos.

Ransomware data de 1989, pero en los últimos tres años ha tenido un gran auge. Millones de computadoras ha sido infectadas y los cibercriminales han lucrado decenas de millones de dólares americanos, gracias al dinero que los afectados les han pagado. Las víctimas son personas, compañías, computadores y dispositivos móviles con sistema operativo MS Windows, IOS y Android. Panamá no es inmune y muchos casos se han dado.

La forma de infectarse se da vía una página web, al dar *click* a un enlace o salvar en su computador o dispositivo móvil un archivo adjunto de un correo no solicitado (spam). Si el computador o dispositivo móvil se infecta con un *Ransomware*, fuera de la frustración, las implicaciones van desde ser improductivo al no poder tener acceso a los documentos y datos, hasta la posibilidad de no poder recuperarlos nunca a pesar que haya pagado el rescate.

Debido a que existen diferentes variantes de *Ransomware*, a la fecha, no existe una cura única. La prevención es la mejor alternativa. Realice copias de respaldo a los datos regularmente y manténgalas *off line*. Eduque a su familia o colaboradores. Lamentablemente, ante la ausencia de una copia de respaldo a los datos reciente y dada ciertas circunstancias, pagar el rescate podría ser su única opción.

Tenga presente que quizás usted como persona no sea atractiva para que criminales lo secuestren, pero sus documentos digitales, seguramente sí.

© 2009 - 2015 RISCCO. Todos los derechos reservados.

2. ¿QUÉ ES *RANSOMWARE* O CIBERSECUESTRO?

Imagínese que enciende su computador o dispositivo móvil, desea acceder a sus documentos o programas y no puede, ya que, en su pantalla aparece un mensaje que indica que sus documentos están encriptados y que tiene 72 horas para pagar entre US$300 y US$6,000 para volver tener acceso a los mismos, o de lo contrario los perderá. Lo anterior se llama *Ransomware* o Cibersecuestro. *Ransomware* es una amenaza creada por bandas de cibercriminales y se deriva de la palabra *Ransom* (rescate) y *ware* (código malicioso).

Esta amenaza data del año 1989 pero se ha hecho popular desde el año 2005. En los últimos dos años ha podido infectar millones de computadores y existen miles de víctimas. Según el sitio en Internet ZDNet, se estima que solo en los últimos tres meses del año 2013, se pagó aproximadamente US$27 millones en recates para poder tener acceso a sus documentos. Existen diferentes variantes de *Ransomware*. Las más conocidas son: *Cryptolocker* y *CryptoWall*, pero en esencia, todas hacen lo mismo.

Finalmente, antes que piense que Panamá es inmune a este tipo de delitos, es sano que conozca que localmente se han dado muchos casos, tanto a personas y organizaciones.

© 2009 - 2015 RISCCO. Todos los derechos reservados.

3. ¿QUIÉNES SON LAS VÍCTIMAS?

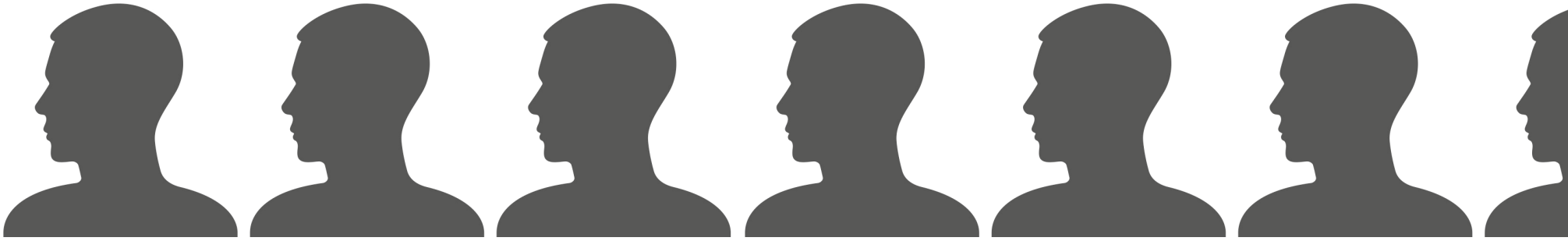
Contrario sensu, el número de víctimas es mucho más de lo que se piensa y son:

- Personas y compañías.
- Dispositivos móviles (Tabletas y teléfonos inteligentes) basados en sistemas operativos IOS, Android y MS Windows Phone.
- Computadoras con sistema operativo MS Windows y Mac OS X.

Entre las formas como el dispositivo (computador o dispositivo móvil) se infecta del *Ransomware*, están:

- Recibir un correo electrónico con un archivo infectado y bajarlo en su dispositivo.
- Recibir un correo electrónico y darle *click* al enlace (*link*) del mensaje.
- Visitar un sitio web infectado.
- Utilizar una misma contraseña para servicios como iCloud y redes sociales o cualquier otro sitio web.

Existe la falsa creencia que esto no afecta a las compañías. Lo cierto es que estás son las más atractivas, ya que, muy probablemente son las que están en la capacidad de pagar el rescate.



© 2009 - 2015 RISCCO. Todos los derechos reservados.

4. ¿CÓMO NOS AFECTA?

Duramente. Aislando la parte sentimental (frustración; molestia; impotencia; ¿Qué hice yo para merecerme esto?; etc.), entre las formas cómo nos afecta están:

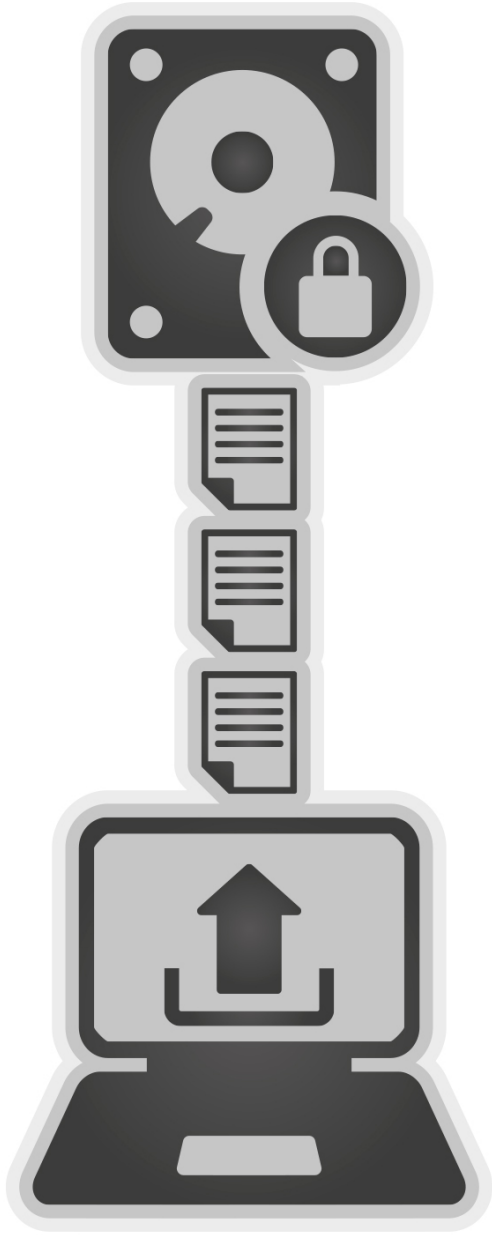
- Improductividad al no poder tener acceso a los documentos de trabajo y programas.
- Pérdida de tiempo al tratar de recuperar los documentos y bases de datos.
- Posibilidad cierta de no poder recuperar nunca los documentos y bases de datos.
- Perder dinero al tener que pagar el rescate.
- No tener acceso a los documentos y bases de datos a pesar que se pagó el rescate.
- Caos en la operación e insatisfacción de los clientes, si no se puede tener acceso a las bases de datos y programas necesarios para la operación de la compañía.

Algunas cosas que debe tener presente en caso usted o su organización sea víctima son:

- No hay garantía absoluta que a pesar que pague el rescate, recupere todos los documentos encriptados.
- El proceso para normalizar las actividades diarias o la operación de la compañía es directamente proporcional a la cantidad de documentos y bases de datos que fueron encriptados. Al menos puede tomar tres días.
- En caso opte que el Departamento de Tecnología o un especialista en seguridad trate de recuperar los documentos y bases de datos, es una tarea que puede tomar varios días sin necesariamente tener éxito.
- Si pago el rescate, no pierda el tiempo en tratar de darle seguimiento al destino de su dinero. Al menos hoy día, estás bandas utilizan preferentemente una forma de pago llamada *Bitcoin*, la cual es anónima y difícilmente rastreable.

© 2009 - 2015 RISCCO. Todos los derechos reservados.

5. ¿QUÉ HACER?



Prevención. Se ha demostrado que la forma más simple y económica de superar un episodio de la amenaza *Ransomware*, es mantener una copia de respaldo de datos y programas reciente. Su ausencia, será especie de una guerra en la cual, tenga la seguridad que aunque la gane (recupere gran parte de sus datos), tendrá bajas.

PRÁCTICAS PREVENTIVAS

- Haga copias de respaldo de datos y programas con regularidad (diariamente) y manténgala *off line*.
- Si es una organización, mantenga las copias de respaldo en un servidor totalmente aislado a los datos en producción.
- Edúquese e instruya a sus colaboradores sobre qué es *Ransomware*.
- No visite sitios en Internet de origen dudoso, no descargue archivos o haga *click* a enlaces recibidos de correos electrónicos no solicitados (*spam*).
- Mantenga actualizado el sistema operativo, programas antivirus y programas navegadores del computador o dispositivo móvil.
- No utilice usuarios con privilegios de administración para tareas rutinarias como navegar por Internet, escribir documentos, leer correos, etc.

EN CASO HAYA SIDO INFECTADO Y TENGA UNA COPIA DE RESPALDO RECIENTE

Restaure su computador o dispositivo móvil a la instalación que vino de fábrica, haga las actualizaciones respectivas de los programas y copie los documentos-datos provenientes de la copia de respaldo.

© 2009 - 2015 RISCCO. Todos los derechos reservados.

EN CASO HAYA SIDO INFECTADO Y NO TENGA UNA COPIA DE RESPALDO RECIENTE

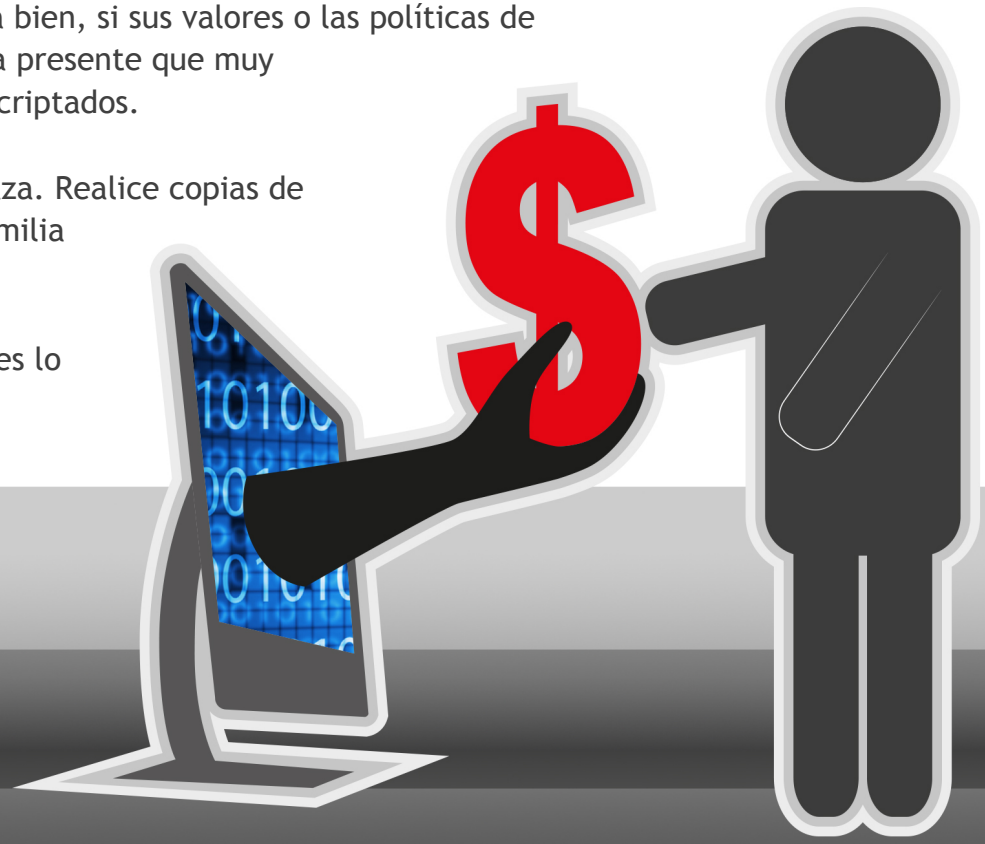
En este escenario, todo va a depender del tiempo y la situación en que se encuentre. La mayoría de los *gurús* y especialistas recomiendan nunca pagar el rescate. Aunque es compresible dicha posición, en ocasiones no es práctica. Si usted tiene documentos importantes o la organización depende de una base de datos para generar ingresos o brindar servicio al cliente, y esta fue infectada con un *Ransomware*, muy probablemente usted prefiera pagar el rescate y reestablecer la operatividad de compañía.

Debido a que existen diferentes variantes de *Ransomware*, a la fecha, no existe una cura única. Hay ciertas tareas que se pueden realizar según la variante de *Ransomware* para tratar de recuperar los documentos y datos, pero toman tiempo y tampoco son garantía.

En función de lo anterior, si el tiempo lo permite, busque posibles soluciones en Internet a la variante que le afecto. En caso no tenga tiempo para tratar de recuperar los documentos y datos encriptados, y en su criterio los mismos valen más que el monto del rescate, considere pagarlo. Ahora bien, si sus valores o las políticas de la organización le impiden negociar con ciberterroristas, tenga presente que muy probablemente no podrá recuperar los documentos y datos encriptados.

La prevención es la mejor alternativa para este tipo de amenaza. Realice copias de respaldo a los datos regularmente, edúquese y eduque a su familia o colaboradores.

Quizás usted como persona no sea atractiva para que criminales lo secuestren, pero sus documentos digitales, seguramente sí.



© 2009 - 2015 RISCCO. Todos los derechos reservados.

CONTACTOS

Antonio Ayala I.
t: 279-1410 Ext. 104
aayala@riscco.com

Benildo Vergara
t: 279-1410 Ext. 105
bvergarad@riscco.com

riscco.com

Es una compañía panameña, independiente y dedicada, de manera exclusiva, a la consultoría en riesgo tecnológico, seguridad de información y auditoría interna, compuesta por profesionales con el conocimiento y credibilidad necesaria para traducir aspectos muy técnicos a un lenguaje simple y con sentido de negocio. Con seis años de haber iniciado operaciones, RISCCO cuenta en su cartera de clientes con compañías privadas e Instituciones del Estado Panameño, líderes en su ramo.

© 2009 - 2015 RISCCO. Todos los derechos reservados.

Desarrollo Gráfico Bellator Creative SAS
bellatorgallery.com – info@bellatorgallery.com