

CIFRADO ASIMÉTRICO - RANSOMWARE¹

M. en .C Ángel Salvador López Vásquez²
angel.vasquez@zicatela.umar.mx

Diciembre 2016

En la actualidad se ha vuelto común mantener la privacidad de la información digital lo más segura posible, la historia relata que hace miles de años tanto los espartanos, griegos y romanos utilizaron diferentes técnicas y métodos para compartir información confidencial cuyo propósito era: que sólo las personas autorizadas pudieran entender el mensaje sin que esta llegara a manos enemigas, creando con ello su propio sistema de cifrado acorde a aquella época. Así que regresando un poco al mundo digital en el que estamos inmersos hoy en día, sabemos que la información es el recurso más importante tanto para las personas como para las grandes empresas, por esa razón es necesario protegerla ante cualquier riesgo. Y es aquí donde el cifrado asimétrico juega un papel muy importante, ya que nos va a permitir modificar de manera eficiente la información utilizando algoritmos matemáticos de cifra que permiten a su vez proteger toda información sensible de una persona o de una organización, con la finalidad de que si los datos son interceptados por terceros, estos no podrían ser leídos por la complejidad de los mismos, ya que el cifrado asimétrico trabaja siempre con un par de claves, una de ellas es la clave pública y la otra es la clave privada, siendo cada vez más difícil descifrar la información. Y bien en dónde entra el “Ransomware”, la mayoría sabemos que aunque el avance de la tecnología y de los sistemas informáticos va en aumento, también sigue creciendo de forma alarmante el robo de información o secuestro de los datos utilizando “Ransomwares” (*virus informático-malware*) el cual utiliza la técnica del cifrado de datos asimétrico para que los usuarios que han sido víctimas no puedan acceder a sus archivos o peor aún no puedan acceder a sus equipos personales como son: computadoras personales,

¹ El presente resumen es un producto final del seminario brindado el 14 de diciembre del 2016 en la Universidad del Mar Campus Puerto Escondido.

² Profesor Investigador de la Lic. En Informática en la Universidad del Mar Campus Puerto Escondido

Ángel Vásquez

computadoras de escritorio, teléfonos inteligentes, tabletas, etc., poniendo en riesgo la información que hay en los mismos. Hasta hace algunos años esto parecía sacado de una película de ciencia ficción, pero hoy podemos observar una infinidad de casos, como es el famoso virus de la policía que se instala en un equipo de cómputo cifrando la información de un usuario y al mismo tiempo pidiendo una fuerte suma de dinero mediante un rescate electrónico que debe ser pagado con tarjeta de crédito, es un hecho alarmante que este tipo de situaciones estén sucediendo y peor aún que puedan implantarse en equipos de grandes empresas ocasionando diferentes tipos de problemas que van desde no poder acceder a cuentas personales, hasta la pérdida de dinero en alguna cuenta de banco. Así que el cifrado asimétrico, al ser tan robusto para proteger la información es imposible acceder a ella si no cuentas con la clave privada, por eso los ciberdelincuentes están aprovechando el cifrado utilizando un poco de ingeniería social en las personas con escasos conocimientos informáticos, y con esto obtienen sumas importantes de dinero.

Por esa razón debemos crear conciencia a la hora de navegar por internet, y evitar descargar aplicaciones para piratear algún software (*incurre en un delito y de paso te instalas de manera gratuita algún malware*), también debemos ser cuidadosos a la hora de abrir algún correo de algún destinatario poco conocido ya que puedes caer en “*Pishing*” (*robo de identidad*) con el simple hecho de hacer clic en algún enlace o descargar y ejecutar algún archivo adjunto. Como conclusión debes tener siempre a la mano un buen software antivirus y algún software antimalware, que permita lanzar notificaciones cuando tu equipo se vea comprometido por alguna de estas y otras amenazas, logrando con esto destruirlas sin mayor problema. Es un hecho que el cifrado asimétrico apoya en la protección de la información, así que hagamos buen uso de esto.

Ángel Vázquez