Ransomware

Wanna Cry, ¿qué es y cómo proteger nuestros equipos?

Por Óscar Gail Martínez López y Juan Miguel Hernández Neri



Ilustración digital: Gerardo Mercado

La distracción y el desconocimiento de los usuarios son los principales causantes de las fallas en los sistemas de seguridad informática; pero no todos son errores, algunos programas son creados especialmente para provocar daño, como el *ransomware* Wanna Cry.

Un ransomware es un código malicioso que toma el control de una computadora, encripta los datos del usuario y luego exige un pago para restaurar el acceso normal al sistema.

El monto del rescate es de 300 a 600 dólares en *bitcoins*, moneda virtual o digital para transacciones en línea. Si no se hace el cargo en el tiempo estipulado, el costo aumenta y no hay garantía de recuperación.

Wanna Cry, WCry, WannaCryptor o WannaDecryptor 2.0 es un *malware*, tipo ransomware, que cifra todos los archivos de las unidades conectadas en red e infecta los sistemas de Windows, mediante la ejecución de comandos desplegados por el protocolo de red Samba (antes SMB), el cual permite compartir archivos, impresoras y otros dispositivos.

Kaspersky, compañía rusa especializada en antivirus, reportó que alrededor de 50 mil computadoras en todo el mundo fueron infectadas.

Entre los más de 70 países que registraron ataques, se encuentran Estados Unidos, España, China, Rusia y el Reino Unido; en este último el sistema de salud fue el más afectado al perder operaciones programadas y modificar citas. México también está este grupo.

Medidas de prevención y mitigación:

- Actualizar el sistema operativo y todo el software a sus últimas versiones.
- Tener instalado un antivirus de alta protección y actualizarlo.
- Hacer un respaldo de la información.
- Evitar hacer clic en los enlaces que parezcan sospechosos; estos pueden ser sugeridos en correo electrónico, redes sociales, aplicaciones, memorias USB y otros dispositivos externos.

Si el enlace viene en el correo de una persona conocida, hay que confirmar con el remitente que efectivamente lo envió. Las computadoras infectadas reenvían correos aleatorios a la lista de contactos con el enlace del malware.

Ya existe una actualización de seguridad contra este malware que se instala desde el servidor de Windows: XP, Vista, Server 2003, Server 2008 SP2 and R2 SP1, 7, 8, 8.1, RT 8.1, Server 2012 and R2, 10 y Server 2016; en el caso de Mac, MacOS.

Si quieres ver los ataques alrededor del mundo en tiempo real puedes consultar este enlace:
https://intel.malwaretech.com/WannaCrypt.html.

Enlaces de interés:
https://technet.microsoft.com/en-us/library/security/ms17-010.aspx
http://www.catalog.update.microsoft.com/Search.aspx?q=KB4012598
http://www.infonort.com/parche-de-seguridad-contra-el-ramsomware-wanna-cry/
https://blogs.technet.microsoft.com/msrc/2017/05/12/customer-guidance-for-wannacrypt-attacks/





Óscar Gail Martínez López, responsable de la Unidad de Informática de la Dirección General de Comunicación Universitaria UAEM, y **Juan Miguel Hernández Neri**, ingeniero de soporte del área de Seguridad Informática de la Dirección de Tecnologías de la Información y Comunicaciones de la UAEM.