Published on *Revista .Seguridad* (http://revista.seguridad.unam.mx)

CIBERAMENAZAS: UNA OPORTUNIDAD EN LA CRISIS. APRENDIZAJES PARA MEJORAR LA SEGURIDAD

revistas:

numero-29

No hay *malware* que por bien no venga. La alarma generalizada que causó el *ransomware* WannaCry alrededor del mundo provocó distintos escenarios de crisis, permitiendo que el tema de la ciberseguridad fuera abordado con preocupación tanto por instituciones públicas como privadas, convirtiéndose en un tema de sobremesa entre familiares y amigos.

Este malware propició que muchos usuarios alrededor del mundo tomaran conciencia sobre medidas de seguridad para resguardar su información y sus dispositivos. Cuando una amenaza afecta directamente a un usuario o a su entorno, se da cuenta del impacto que puede provocar en su vida.

El famoso *ransomware*, que provocó el cierre de hospitales e interrumpió la operación de negocios, no es la única amenaza. En un reporte a cargo de McAfee sobre el primer trimestre de 2017, se asegura que se detectaron 32 millones de muestras de malware. En términos generales, se descubrieron 244 amenazas por minuto, es decir 4 amenazas por segundo. El número de ciberamenazas crece como resultado de la sofisticación de ataques, y en respuesta al aumento de dispositivos conectados a Internet. Recientemente, se ha sonado también la alarma ante otros malwares como Petya, Pegasus o Fireball.

Por ello, en este número se abordan distintas temáticas cuyo propósito es alentar a los responsables de seguridad a ver en las crisis una oportunidad para tomar acciones y hacer frente a las crecientes amenazas, en un ambiente en el que los profesionales de la seguridad son cada vez más requeridos.

La **seguridad en la nube** es un tema importante, pues muchas organizaciones están migrando su información, sus sistemas e infraestructura a algún servicio resguardado por un tercero; también se aborda cómo se implementa la ciberseguridad en las **Instituciones de Educación Superior**, y se invita a incorporar las políticas necesarias para disminuir los incidentes; además se habla sobre cómo la **experiencia de usuario**

puede apoyar a la ciberseguridad, en específico en la interacción con la banca electrónica.

Adicionalmente, publicamos un artículo sobre ***macro malware***, una técnica que aprovecha las macros de los archivos ofimáticos para lanzar ataques, y cuya incidencia ha aumentado en nuestro país. Por último, se ofrece una guía para usar **Conpot**, un Honeypot que permite recolectar inteligencia sobre los métodos, técnicas y motivos de los ciberdelincuentes cuyo objetivo son los Sistemas de Control Industrial.

Las amenazas podrán multiplicarse, pero una actitud defensiva y proactiva permitirá afrontarlas para mantener nuestro entorno seguro.

UNAM-CERT

Source URL: http://revista.seguridad.unam.mx/numero29/editorial