LA RAZÓN

25 de enero de 2017

Diez ciberdelitos que temer este año

Hoy termina el 50º Congreso TF-CSIRTE en Valencia, probablemente el más importante a nivel mundial en cuanto a ciberseguridad. Allí se han discutido las tendencias a las que expertos y usuarios debemos estar atentos. «Se prevé que este año –explica Miguel A. Juan, del S2 Grupo, firma valenciana especializada en ciberseguridad– estará marcado por ataques que supongan un gran beneficio económico para el "hacker" basados en "ransomware", ataques para compra y alquiler de capacidades o destinados a los directores financieros de las entidades». También se habla de atacar dispositivos médicos como una tendencia cada vez mayor. En este sentido InnoTec (Grupo Entelgy) ha elaborado una lista de los 10 ciberdelitos que más sufriremos.

SECUESTRO EXPRÉS O «RANSOMWARE»

Se trata de un «malware» que el usuario descarga en su ordenador sin darse cuenta. Inmediatamente después, el «hacker» comienza a acceder al dispositivo para saber nuestros usos más habituales y bloquear los archivos que consideramos imprescindibles. A cambio de una suma de dinero, el «hacker» puede liberar estos archivos.

UN VIRUS MODERNO

Desde hace relativamente poco los expertos en seguridad han comenzado a detectar un tipo de «malware» que actúa sin un archivo: el afectado no necesita descargarse nada para verse afectado, algo que lo hace sumamente elusivo y difícil de detectar.

SU RED ESTÁ DENEGADA

Los ataques DDoS (siglas de Denegación de Servicio) se basan en solicitudes masivas que hacen caer una red. Cuanto más importante, mejor. Es como si enviaran tantas cartas que un buzón ya no puede contener más y explota, sólo que a nivel digital. El año pasado los ataques DDoS se duplicaron.

ATAQUES CEBO

Cuando se realiza una compra en la web, la mayoría de las empresas utilizan el protocolo HTTPs, gracias a él la web codifica la sesión y la información comienza a encriptarse. El problema es que los «hackers» han encontrado un modo de burlar este protocolo y fingir que se trata de páginas seguras. Este tipo de delitos se ha multiplicado por cinco en 2016.

MALDITA PUBLICIDAD

Otra moda reciente (la primera fue detectada en 2015) consiste en utilizar publicidad digital que parece legítima para que el usuario se descargue «malware».

PERSONALIDAD MÚLTIPLE

Ya no sólo se trata del robo de la identidad de personas («pishing») sino también comienza el auge del «spearphishing». Son páginas web que directamente fingen lo que no son: bancos, empresas y servicios se verán afectados por esta tendencia, también en aumento.

CARA A CARA

Cada vez son más los casos de «ciberdelincuencia retro». En lugar de atacar al ordenador o al móvil, llaman por teléfono para, con la excusa de una oferta o de un premio, obtener nuestros datos.

EN LA NUBE

Poder acceder a nuestros archivos desde cualquier dispositivo es una ventaja indudable… para nosotros por comodidad y también para los «hackers», por los mismos motivos. Los expertos anuncian que este año los servicios en la Nube sufrirán importantes ataques.

MÁS PUNTOS DE ATAQUE CON LA IRRUPCIÓN DEL INTERNET DE LAS COSAS

La irrupción del Internet de las Cosas (IoT), la conectividad de sensores, dispositivos y electrodomésticos entre sí y con la red, será también un objetivo muy preciado por los ciberdelincuentes.