Internet y nuevas tecnologías

ROBERTO PLÁ
Coronel de Aviación
http://robertopla.net/

HACKING

OTRO HACKEO DE UNA WEB DE CONTACTOS

Hace unos meses en esta misma sección comentábamos el hackeo de la web de contactos Ashley Madison, que provocó la embarazosa exposición de los datos de 32 millones de usuarios, lo que ya resultaba una cifra abrumadora. Poco podíamos sospechar que un año después, otra web de contactos sería víctima de un hackeo que ha comprometido los datos de diez veces más usuarios que aquel caso, estableciendo un nuevo triste record.

La web hackeada ha sido Adult FriendFinder, una web líder en el campo de contactos entre adultos y que cuenta con millones de personas suscritas en todo el mundo. Nada menos que 339 millones pueden haber visto comprometidos sus datos en el incidente que la compañía reconoció haber sufrido el pasado 14 de noviembre, que afecta también a otras webs de la compañía e incluso a 15 millones de cuentas de usuarios que se habían dado de baja, pero cuyos datos no se borraron.

Adult FriendFinder se denomina a sí misma como "la comunidad más grande del mundo de sexo y libertinaje" y el pasado año ya sufrió un robo de información que afectó a tres millones y medio de cuentas de las que los hackers obtuvieron todos los detalles, incluidos los más íntimos que puedan revelarse en este tipo de webs. En este caso parece ser que los hackers solo obtuvieron información sobre la identidad, correo electrónico y claves de acceso de los usuarios.

Más allá del chascarrillo social, la auténtica importancia de estas acciones, desde el punto de vista de la seguridad es el peligro que supone para los usuarios que esos datos estén en el mercado de la delincuencia digital.

Si el número de nuestra tarjeta ha pasado a poder de grupos de moral dudosa, hay que pensar en que hay países en los que basta con el número de la tarjeta de crédito para hacer compras.

Si lo que hemos perdido es la clave de acceso hay que tener en cuenta que hay muchos usuarios que usan la misma clave para varias cuentas. Si la clave no se cambia antes de que los hackers encuentren esas cuentas, podrían perder más datos y comprometer, por ejemplo su lista de contactos en un sistema de correo público como Hotmail, Yahoo, o Gmail.

Finalmente, aunque el botín solo incluya millones de direcciones de correo, se trata de una información, que en manos de los indeseables adecuados, puede convertirse en dinero fácilmente, al venderse para remitir spam o realizar ataques de phishing. Si el correo va asociado con los datos bancarios o la tarjeta de crédito, el ataque derivado puede ser más sofisticado, ya que la mayoría de las veces lo que el phishing pretende es hacernos creer que es nuestro banco quien nos escribe para forzar a que introduzcamos nuestro nombre de usuario y clave en una web falsa, donde los delincuentes son los que reciben la llave que da acceso a nuestras cuentas.

Estos ataques están dirigidos al punto más débil de cualquier sistema: el usuario. Aunque la formación y la prudencia de los usuarios crece con la digitalización, cuando se disponen de millones de direcciones, basta que un porcentaje mínimo sean usuarios poco prudentes, para obtener un buen número de víctimas a las que desvalijar.

El mejor consejo para evitar estas situaciones (además de evitar las webs de 'dudosa' reputación...) es utilizar claves diferentes para cada servicio web o aplicación que utilicemos y cumplir las recomendaciones de desconfiar de cualquier archivo no solicitado que nos llegue por correo, y no seguir los enlaces que llegan en un correo aunque pueda parecernos que es de una persona de confianza. Porque la confianza (también) mató al gato.

DISPOSITIVOS MOVILES

TELÉFONOS CHIVATOS

También se ha mencionado en esta sección el peligro que representa el software integrado en dispositivos que usamos a diario pero que no podemos desinstalar, ni sabemos como funciona. Se trata del firmware, un código que en el caso de los teléfonos puede hacer de todo con nuestro terminal, incluso con nuestra tarjeta de abonado al servicio telefónico sin que podamos evitarlo. De hecho sin que pueda evitarlo ni siquiera el sistema operativo del teléfono.

Cuando se examina minuciosamente el contrato de usuario de algunos terminales económicos procedentes de China, se descubre con sorpresa que aceptamos que la compañía fabricante del teléfono proporcione “algunos datos” sobre el uso que hacemos del mismo...

¡al Gobierno de la República Popular de China!

Pero hace poco, un analista de la empresa norteamericana de seguridad Kryptowire descubrió que un teléfono económico de la marca BLU tenía una actividad sospechosa. Tras analizar sus comunicaciones se descubrió que enviaba datos sobre movimientos, llamadas y otros detalles del teléfono a un servidor en Shanghai y estaba registrado por Adups, fabricante del firmware del teléfono.

Adups trabaja para varias de las principales compañías fabricantes de teléfonos móviles en China y al parecer había introducido esa 'peculiaridad' en su código a petición del Gobierno chino, según dicen, para los teléfonos de uso interno, aunque incluyó la misma versión del software 'chivato' en los terminales destinados a la exportación.

Más de 200 millones de dispositivos inteligentes utilizan su software en todo el mundo. Aunque el escándalo ha sido descubierto en teléfonos de la marca BLU vendidos en norteamérica, puede afectar a muchas marcas chinas, como Huawei, que se ha apresurado a comentar que no está afectada y que sus terminales no incluyen esas características.

Curiosamente Huawei abandonó el mercado norteamericano en 2013 ante los rumores de que facilitaba el espionaje chino, para descubrirse un tiempo después que sin embargo habían sido víctimas de espionaje por parte de la NSA desde hacía al menos tres años.

INTERNET

INTERNET DE LAS COSAS Y LA INDUSTRIA

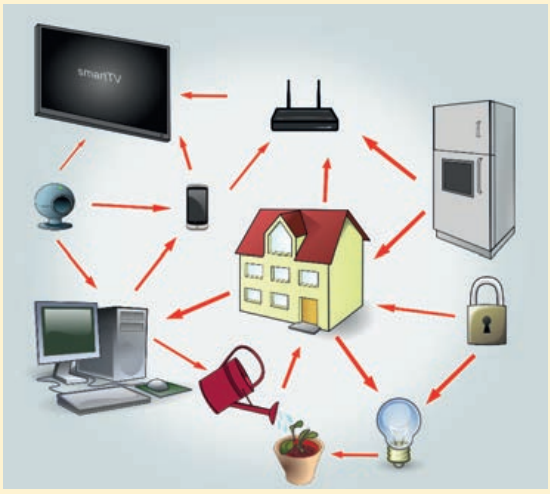
El pasado mes de octubre se celebró en Barcelona el congreso mundial del internet de las cosas, "IOT Solutions World Congress" al que han asistido más de 8.000 visitantes de 70 países para escuchar a 160 conferenciantes y ver lo que se mostraba en los stands de 170 compañías.

El evento, organizado por Fira Barcelona en colaboración de Industrial Internet Consortium, (la organización industrial IoT fundada por AT&T, Cisco, General Electric, IBM, e Intel) ha tenido como objetivo mostrar a la industria la tecnología disponible, con el objetivo de acelerar el crecimiento, la adopción y el uso generalizado de la IoT industrial. El Internet de las cosas es probablemente uno de los sectores industriales con unas mayores expectativas de crecimiento en un futuro próximo.

Para un visitante profano la feria no era excesivamente atractiva. La oferta se dividía entre las empresas que presentaban soluciones propietarias en sensores y elementos físicos para la implementación de automatismos y conexiones, el software para controlarlas o ambas cosas a la vez.

También había un sector importante que mostraba las posibilidades de elementos estándar de bajo coste y estándares abiertos utilizados para proyectos de envergadura. Me refiero a diferentes combinaciones de Arduino y todos sus complementos comerciales, desde gps a tarjetas para conexión a la red telefónica móvil o de red, pantallas y sensores de todo tipo, frecuentemente controlados por pequeños servidores implementados en placas de PC ultra miniaturizados como Raspberry Pi y otros similares.

Estos elementos son accesibles y baratos en el mercado y a mi modo de ver van a constituir uno de los puntos clave del crecimiento del sector.



Entre las cosas que llamaban la atencion en la feria, cuando se pasa de la impresion inicial de la multitud de visitantes y de exposiciones poco expectaculares, estaba el sistema de control de mantenimiento de los motores de aviación Rolls&Royce, presente en el stand de Microsoft cuyo entorno Azure IoT Suite, la solucion que la compañia de Windows ofrece para conectar dispositivos, analizar datos previamente no explotados e integrarlos en la gestión empresarial o crear nuevos modelos de negocio.

En el caso de los motores denominados 'inteligentes' de la prestigiosa firma británica, se mostraba la gestión de datos tales como los de la salud del motor, información sobre el control del tráfico aéreo, las restricciones de rutas y datos de uso de combustible que se recogen en tiempo real para detectar anomalías y tendencias operativas, para luego poder proporcionar información detallada sobre su desempeño, resultados y acciones de mantenimiento necesarias, accesibles tanto para la tripulación y aplicaciones móviles como para la compañía operadora, el servicio de mantenimiento o el fabricante, a través de internet.

Los testbeds son plataformas de experimentación pensadas para aplicar nuevas soluciones y testearlas en condiciones reales de funcionamiento. En el congreso se presentaron diez de ellos, uno de los cuales denominado "Smart Airline Baggage Management", mostró cómo General Electric, Oracle, Infosys y M2MI han creado una solución para reducir las pérdidas de maletas y los daños en el equipaje en los aeropuertos. El testbed fusiona varios sistemas de Internet de las cosas localizando y conectando maletas, handling, transporte y gestión del equipaje del aeropuerto (rampas, camiones, seguridad, aviones, etc.). De este modo, se pretende reducir los 23 millones de maletas perdidas cada año en los aeropuertos y reducir los gastos de indemnización que comportan.

Ni que decir tiene que una de los principales aspectos a considerar del IoT es la seguridad. Su importancia es tal que a la participación de estos dispositivos en los últimos incidentes de ataques masivos, tendré que dedicar un artículo en un próximo número. •