Ciberriesgo para particulares

Manuel Huerta

12345, todos aquellos que han respondido con una sonrisa al leer esto, ya saben de qué estamos hablando, para todos aquellos que no, simplemente comentar que es la contraseña más utilizada del mundo.

Hace muy pocos años, podíamos hablar de dos grandes grupos de usuarios (incluidas empresas), los que habían sido atacados y los que no, en la actualidad siguen existiendo dos grandes grupos de usuarios que se diferencian de la anterior clasificación por un pequeño matiz, los que lo saben y los que no.

Esta diferencia entre haber sido atacado y saberlo, nos indica, cómo en pocos años se puede afirmar con rotundidad que todo el mundo ha sido atacado, sin tratar de sembrar el pánico hemos de matizar que estos ataques afortunadamente tienen más tasa de fallo que de éxito, pero cuando son exitosos producen un efecto mediático muy alto.

Aún existiendo esta tasa de fallo, nada mas lejos de desalentar al ciberdelincuente, los ataques se incrementan todos los años

tanto en los vectores de ataque como el número de los mismos. Desmoralizar o desalentar a alguien que se pone en marcha con el fracaso por delante es muy complicado, tan complicado que sabe desde el principio que lo va a intentar el numero de veces que sea necesario, hasta conseguir una cosa, que el que falle sea el usuario.

En un escenario en el que los riesgos tienen múltiples naturalezas, riesgos laborales, de circulación, sanitarios, la labor informativa que se ha realizado en cada uno de estos campos ha sido tan intensa y continuada que prácticamente todo el mundo sería capaz de enumerar un decálogo de precauciones para cada una de estas áreas, pero ¿qué sucede con nuestro entorno tecnológico?

El entorno tecnológico ha conseguido un factor de penetración tan vertiginoso, que la sociedad se ha limitado a adoptarlo rápidamente por los factores facilitadores, sin sopesar los tipos de riesgo que puede acarrear. Es conocido por todos, el riesgo de manejar un vehículo de manera inapropiada, pero no conocemos el riesgo del manejo inadecuado no ya de nuestros dispositivos tecnológicos, sino de nuestro entorno tecnológico general.

Uno de los principales factores que influyen en esta situación, es la falsa sensación de seguridad derivada de la custodia física, detallemos un poco más este punto.

Como norma general, excepto despistes, podríamos entender como protocolo de seguridad nuestro procedimiento para salir de casa o aparcar el coche, apagamos luces, comprobamos que todo esté cerrado, bajamos persianas, echamos la llave, ponemos la alarma y nos guardamos las llaves, todo bajo control «tenemos las llaves en el bolsillo», lo mismo sucede si aparcamos el coche, cerramos ventanas, bloqueamos el coche y nos guardamos las llaves en el bolsillo, probabilidad de que nos roben en casa o nos roben el coche, con todo cerrado y las llaves en el bolsillo: menos que si dejamos todo abierto y las llaves puestas.

Qué pasa con los dispositivos tecnológicos, ¿está seguro por que los llevamos en el bolsillo o en la mochila? Qué comprobaciones de seguridad hemos efectuado antes de guardarlo, al igual que hacemos con la casa o el coche? Probablemente ninguna.

Hemos de ser conscientes de que nuestros dispositivos, especialmente los móviles, que son los que mas información personal contienen, están permanentemente conectados.

Evidentemente, y lejos de querer ser alarmista, el mero hecho de que los dispositivos estén permanentemente conectados, no es un riesgo en sí mismo, si se toman determinado tipo de medidas tan sencillas y cotidianas como las que tenemos al salir de casa o aparcar el coche.

Los factores que influyen en la posibilidad de ser parte del objetivo de un ataque, vienen derivados de cómo funcionan los sistemas de información, ya que no sólo sirven información, sino que también la recopilan. Para los menos familiarizados con las mal llamadas nuevas tecnologías, (Internet tiene ya 50 años), la Informática se forma a partir de «información y automática», por lo que automatizar cualquier proceso, incluido un ataque de cualquier naturaleza, se puede realizar sin muchos medios.

Antes de explicar cómo se puede preparar este entorno para automatizar una recopilación de datos para un ataque, vamos a pasar a exponer los riesgos más comunes para los usuarios particulares, finales o domésticos, ya que la naturaleza de los ataques empresariales tiene otros objetivos.

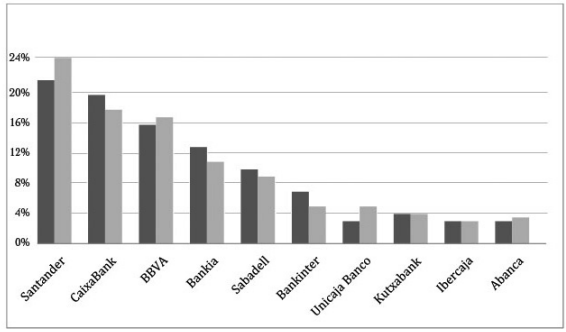
Al igual que la delincuencia tradicional, la ciberdelincuencia también tiene grupos especializados, siendo el trasfondo económico el objetivo común del que existen muchas maneras de obtenerlo como vamos a ver a continuación, empezando por las más directas hasta las más indirectas.

Una de las que más crece es el *phishing*, que consiste básicamente en una suplantación de la identidad de una entidad bancaria

o de cualquier otro medio de pago, que permite al delincuente hacerse con las claves para operar en ese medio, engañando al usuario haciéndole creer que está interactuando con su entidad, pero en realidad cuando éste introduce sus claves, se las esta facilitando al ciberdelincuente, de manera que éste con posterioridad procederá a retirar las cantidades de dinero que le sea posible de cada una de las cuentas de las que consiga las claves.

La manera mas habitual es recibir algún tipo de aviso por *email* o sms, perfectamente formateado para parecer legítimo, incluso incluyendo advertencias de seguridad respecto a no facilitar las claves. Aunque pueda parecer increíble que haya mucha gente que caiga en este tipo de engaños, en realidad la efectividad de este tipo de campañas es muy baja porcentualmente en relación a la volumetría del ataque, pero hagamos una pequeña disección de los datos:

Si partimos de una base de 2,5 millones de direcciones electrónicas, que previamente se han filtrado por su origen, si el destino es España se seleccionaran preferentemente correos que se conozca que son españoles, o que terminen en «.es», ya que si el ciberdelincuente va a realizar una campaña contra clientes del RBS (Royal Bank of Scotland) las probabilidades de que un correo terminado en «.es» tenga una cuenta, son muy bajas. En cambio, por *share* de mercado es mucho más probable que tenga cuenta en alguna de las entidades españolas.



Como vemos en el gráfico, el porcentaje de cuota que tenemos por cada banco, nos da unas posibilidades estadísticas, en primer lugar, el receptor debe tener cuenta en la entidad que se quiere suplantar y en el peor de los casos según el grafico es un 5 por ciento aproximadamente.

Por lo que tendremos un objetivo aproximado del 5 por ciento en la base de datos de 2,5 millones de correos, 125.000 objetivos potenciales, de los cuales un alto porcentaje de los correos van a ser clasificados como *spam* por el servicio de correo electrónico. De los correos que pasen los filtros de *spam* y que van a llegar a su destino, si bien la mayor parte de los usuarios los descartarán, existe un porcentaje que sugestionado por las advertencias del mensaje seguirá el enlace y ante la apariencia de autenticidad introducirá sus claves. Un ratio de efectividad del uno por mil, implica la exposición de 2.500 credenciales bancarias en este caso.

De media los sistemas bancarios conseguirán detectar dos tercios de las operaciones fraudulentas, bien por origen de la conexión, IP, por el destino de los pagos, y otros sistemas de inteligencia y análisis. El tercio restante sufrirá una retirada de fondos que no podrán recuperarse, con importes de entre 600 y 10.000 euros como promedio, tendríamos una operación de 833.000 euros de fraude. Los datos medios que declaran como impacto las entidades bancarias, duplican de media esta cantidad alcanzando, 1,6 millones de euros como impacto medio por cada campaña de *phising*.

Este tipo de campañas afectan además de a Bancos, a entidades de pago como emisoras de tarjetas de crédito, Visa, Amex o medios electrónicos, como Applepay, Samsung Pay, Paypal, etc.

El siguiente gran foco de la ciberdelincuencia enfocada en particulares es la extorsión. La mas conocida por el impacto que ha tenido los últimos años y su factor de crecimiento ha sido el *ransomware* (secuestro de información), aunque expondremos otras

formas de extorsión más adelante, comenzaremos explicando cómo funciona el *ransomware*.

El método de dispersión más habitual de este tipo de ataques es el correo electrónico, aunque también se engrosa el número de infecciones mediante páginas web comprometidas.

Lo mas habitual es recibir un correo electrónico, parecido al del *phishing*, simulando ser una entidad que envía un documento, el cual contiene código malicioso o bien un enlace para consultar algún servicio relacionado con el objeto del correo, siendo los mas habituales proveedores de servicios online, redes sociales, empresas de transporte, fabricantes de tecnología como Apple o Samsung. En el mismo instante que abramos el documento o accedamos al enlace, se comenzara a ejecutar en el ordenador un proceso de encriptación que afectara sólo a la información mas común, es decir ficheros ofimáticos, fotos, audio, video, correo electrónico, procurando siempre que el ordenador continúe funcionando correctamente para garantizar la posibilidad de cobrar el rescate.

El tipo de cifrado dependerá de cada tipo de ataque, pero siempre tendrá la robustez necesaria para que no sea sencillo recuperar la información cifrada sin pagar el rescate.

Si se tiene la costumbre de realizar *backups* habitualmente y siempre que éste no este conectado en el equipo infectado, podremos restaurar la información sin pagar el rescate, por lo contrario y más habitual, en caso de no disponer de *backup*, la posibilidad de recuperar la información encriptada sin pagar al secuestrador pasa ineludiblemente por acudir a un especialista en recuperación de datos, que dependiendo de la cepa del *ransomware*, puede disponer o no de solución, siendo un servicio que va a tener coste si bien gran parte de las compañías de seguros tienen incluida en sus pólizas de hogar la cobertura de recuperación de información. En cambio, en caso de no tener solución, sólo queda dar por perdida la información o bien pagar el rescate.

Es importante destacar que multitud de compañías en todo el mundo, tratan casos de secuestros de información y que siendo muy compleja la solución de estos casos, en gran parte de las ocasiones se consiguen generar procedimientos de reversión o recuperación por lo que recomendamos conservar la información encriptada con el fin de poder aplicar futuras soluciones de reversión.

Los secuestros de información de este tipo, suelen reivindicar el pago de entre 300 y 600 dólares, cantidades que se suele incrementar en el caso de empresas a pagar generalmente en *bitcoins*, lo cual representa una dificultad añadida, ya que para quien no esté familiarizado con los procesos de compra de las criptomonedas, no es nada sencillo de llevar a cabo, dado que requiere de unos procesos de seguridad muy exhaustivos en entidades que no son conocidas por la mayor parte de usuarios. Aun en el caso de conseguir comprarlos, habría que realizar el pago al *wallet* del secuestrador (el *wallet* es el equivalente a una cuenta bancaria en el entorno de las criptomonedas) y esperar a recibir el código de desencriptación, lo cual no sucede una vez realizado el pago en el 40 por ciento de los casos.

Si somos de los afortunados que tras realizar el pago recibimos un código de desencriptación, nos queda la tarea de desencriptar la información, (y limpiar el equipo que, recordemos, sigue infectado) lo cual tampoco es una tarea con la que un usuario domestico este familiarizado y tener que acudir a profesionales (los cuales tampoco todos están familiarizados con este tipo de procesos) se hace casi imprescindible.

Este tipo de ataques, afectan principalmente a plataformas Windows sobre PC, pero también se han visto campañas de secuestros de información en plataforma Apple y en menor medida para Android, especialmente en tablets, mediante páginas web infectadas.

El caso mas famoso de este tipo de secuestros, sucedió hace unos años, conocido como el virus de la policía, que mantenía la maquina secuestrada en cuanto a funcionalidad, pero no afectaba a ninguno de los datos contenidos, y la dispersión fue principalmente mediante paginas web infectadas. En aquella ocasión, sólo en España se registraron más de 700.000 denuncias, sin tener datos exactos de cuántos realizaron el pago, que en aquella ocasión eran 100 euros.

La ultima novedad en los casos de extorsión, consiste en enviar un correo tipo indicando que el ordenador y las claves han sido hackeadas, ofreciendo en el propio correo información sobre las claves sustraídas para darle veracidad, solicitando una cantidad de dinero a cambio de no publicar entre todos los contactos contenido delicado del usuario.

El uso en este caso de una contraseña que es familiar para el usuario, produce un efecto de credibilidad que invita a realizar el pago que se solicita, que suele quedar por debajo de los 300 dólares mediante *bitcoins*.

La fuente de este ataque no es otra que el análisis de las grandes filtraciones de credenciales que se acumulan a lo largo de los años. De estas filtraciones de credenciales se extraen mediante la automatización de las consultas, un correo electrónico junto con las contraseñas que ha filtrado y de esta manera automatiza el envío de correos.

Por lo que, en todos los casos, esta afirmación de haber sido *hackeados* es completamente falsa y no existe el material comprometido que se indica en el correo.

Conviene explicar, que en muchos casos la contraseña a la que hacen referencia en el correo de extorsión, ni siquiera coincide con nuestra contraseña habitual, en muchas ocasiones es una contraseña para algún servicio de prueba que hemos establecido, o alguno que hemos cambiado hace años, por lo que, si por un casual

recibimos el correo indicando una contraseña en uso, por mera precaución deberíamos cambiarlo en aquellos servicios en los que la tengamos en uso.

Como comentábamos anteriormente, iríamos avanzando desde los métodos económicamente más directos a los más indirectos, en los que el afectado no sabe que lo está, pero contribuye de manera indirecta al enriquecimiento del ciberdelincuente.

Botnets, túneles y *malware* publicitario. Estas tres modalidades implican una infección de un equipo que va a realizar una serie de acciones a petición del ciberdelincuente, por la que por supuesto va a percibir beneficios.

Las *botnets*, son redes de millones de ordenadores que están infectados con un software que permite controlarlos para realizar cualquier acción con ellos, tales como ataques de denegación de servicio a un tercero. Mientras el equipo no está bajo el control del operador, éste funciona con total normalidad y la infección no es sencilla de detectar, ya que además no realiza avisos o solicitudes al dueño del equipo. En caso de que se produzca un ataque masivo y éste sea investigado policialmente, nuestro ordenador infectado figurará como participante, por lo que puede repercutir en problemas legales, de aquí que haya que eliminar el pensamiento «yo no le intereso a nadie» o «en mi ordenador no hay nada interesante», el control del equipo es el interés en sí mismo por lo que hay que abandonar esta línea de pensamiento y ser conscientes de los problemas que puede acarrear este tipo de infecciones.

Los túneles, son otro sistema de infección en el que el ordenador es utilizado con distintos fines, y sin que el usuario sea consciente. En este caso, se utilizan los ordenadores infectados para enviar y almacenar información ilegal, como credenciales robadas, tarjetas de crédito o pornografía infantil.

El ordenador infectado, mediante carpetas ocultas almacena información que enviará a otro sitio o establecerá un túnel de co-

municación para realizar los envíos de información de manera que en una investigación será este ordenador y su usuario el que figurará tanto en la tenencia del material como en su difusión, siendo el problema legal en este caso de bastante envergadura, produciendo un gran impacto tanto en la parte emocional del afectado como económicamente por los gastos legales que implica.

El *malware* publicitario, esta versión de un virus busca la generación de trafico y datos publicitarios para engrosar los resultados de las campañas, siendo un fraude para quien contrata la campaña, y aportando beneficio a quienes consiguen grandes redirecciones de trafico a *webs* que realmente no se visitan por parte del usuario, obteniendo el consiguiente aumento de visitas, *clicks*, etc. Habitualmente este tipo de *malware* suele venir incrustado en pequeñas aplicaciones de fuentes dudosas y de cualquier naturaleza, *drivers* ilegítimos de algún tipo de componente, aplicaciones para convertir pdf, visores de video, *plugins* para navegadores.

En ultimo lugar no por ser menos habitual ni menos importante, nos encontramos con los ataques a la intimidad, el honor y la reputación. Aunque términos como el *cyberbulling, sexting, stalking* o delitos contra el secreto de las comunicaciones, se suelen relacionar mas habitualmente con entornos adolescentes, los delitos contra la privacidad de las comunicaciones están cada vez más presentes en entornos domésticos.

El *sexting,* consiste en el envío y la solicitud de imágenes, habitualmente mediante plataformas de mensajería para teléfonos móviles. Si bien en origen este tipo de acciones no necesariamente es un acto delictivo, este tipo de actitudes acaban en una deriva chantajista de una de las partes, que en el momento que deja de consentirse sí pasa a ser un delito en sí mismo.

El acoso o *stalking,* se presenta cuando hay un acoso constante de una persona que vigila, persigue, y contacta con otra a través de medios electrónicos afectando su vida cotidiana, más

conocido también en entornos adolescentes, se da como componente de la violencia de género, ya que estas muestras de acosos y control se convierten en medio de prueba si se judicializan estas situaciones. Las circunstancias de acoso en entornos escolares han tenido en ocasiones fatídicos desenlaces antes la presión sufrida.

El secreto de las comunicaciones, cinematográficamente habitual en las centrales de inteligencia, películas y series de espionaje, pero sin ir más lejos los entornos domésticos en situaciones de violencia de genero y divorcios, presentan cada vez más situaciones en las que un componente de la pareja espía al otro mediante la instalación en el móvil del otro de aplicaciones que nos ofrecen información y datos del dispositivo, como llamadas, posición, mensajes de texto, incluso algunos son capaces de grabar las conversaciones telefónicas y enviarlas a un tercero. En estas ocasiones, cuando el cónyuge realiza la acción movido por los sentimientos no es consciente de la gravedad penal que esto supone, ni que esto conlleva penas de cárcel.

Aparte de todos los riesgos directos relacionados con nuestros dispositivos y la gestión de los mismos, cualquiera de los servicios que utilizamos habitualmente, Google, Spotify, Dropbox, Facebook o Linkedin, entre muchos otros, no dejan de ser un objetivo suculento para la ciberdelincuencia. Es importante destacar para el lector, que los grandes servicios de Internet, disponen de grandes equipos que vigilan la seguridad de la información en todo momento y que controlan los efectos de cientos o miles de ataques diarios con éxito.

Hemos de prestar atención al aumento continuo de dispositivos conectados en nuestro entorno, los riesgos ciber no sólo se limitan al móvil o al ordenador, altavoces inteligentes que están continuamente escuchando para poder recibir instrucciones, Smart Tv (con cámara y micrófono), robots aspirador que mapean nuestra casa e incluso tienen cámaras, equipo domótico que sen-

soriza nuestra casa, video porteros wifi que nos permiten atender o incluso abrir la puerta remotamente, son sistemas con los que ya se convive habitualmente y no van a hacer otra cosa que crecer en implantación, por lo que se hace imprescindible que el usuario comience a concienciarse de la importancia de tomar medidas respecto a las cuestiones de seguridad tecnológica, evitando contraseñas por defecto o poco robustas.

Una vez que hemos explicado los incidentes más comunes, retomaremos la explicación de cómo se organiza y se prepara un ataque desde la automatización de la recopilación de datos.

Teniendo en cuenta que podemos conocer los rangos de IP asignados por IANA (la organización internacional que gestiona la asignación de IP, Internet Assignement Network Authority), podemos automatizar la petición de recursos a los rangos de IP conocidos, es decir básicamente preguntamos a todas la direcciones IP de un rango concreto si dispone de un recurso concreto, por ejemplo preguntar si hay un servidor web detrás, o un puerto concreto relacionado con alguna vulnerabilidad; en la delincuencia tradicional es el equivalente a llamar al timbre de todos los pisos de un edificio de apartamentos, para, en función de que conteste o no conteste, cada uno decidirá qué piso sería el objetivo.

A diferencia de la delincuencia tradicional, esto se puede hacer desde muchos miles de kilómetros de distancia y no limitarnos a indagar sobre un edificio, si no sobre una ciudad o un país.

La forma en que la ciberdelincuencia recopila posibles datos sobre nosotros, no depende únicamente de estas técnicas, en muchas ocasiones sólo necesitan recabar la información que nosotros mismos publicamos, opiniones, post, redes sociales, perfiles profesionales y que puede ser dirigida a perfeccionar cualquiera de los modelos de estafa que hemos explicado anteriormente.

La vertiginosa situación en la que se detectan nuevas amenazas a diario, hace muy difícil para el ciudadano o el usuario final man-

tenerse al corriente de todas ellas y protegerse, pero la adopción de patrones de seguridad y sobre todo de observación, permitirán al usuario alejarse de estas situaciones de riesgo basadas en el engaño.

Las labores de concienciación sobre la importancia de mantenerse alerta y abandonar la idea de la falta de interés para terceros como justificación para no tomar precauciones, es la gran barrera pendiente en la seguridad informática.

Relacionado con la llamada a la sensatez en la gestión de los dispositivos por parte de los usuarios, afrontamos nuevos retos en cuanto a nuestra identidad digital. Al igual que los ciberdelincuentes son un riesgo remoto, las redes sociales e Internet en general, permiten conocernos remotamente sin intenciones ilegitimas, si bien cada vez más tanto las empresas como los departamentos de recursos utilizan estos medios para recabar información sobre los candidatos a un puesto de trabajo, que al exponer ideologías políticas, acciones cuestionables, discusiones abiertas con posturas de todo tipo, acaban conformando un volumen de datos sorprendente, con el que perfectamente se puede construir un perfil razonablemente certero sobre alguien, con el peligro de que, por ejemplo, sea descartado en un proceso de selección por un solo *post*; un me gusta en un sitio políticamente incorrecto, puede dar al traste con una oportunidad laboral. La gestión de nuestra identidad digital también ha de hacerse con determinadas pautas, ya que nuestra identidad digital es también nuestro patrimonio y al igual que no maltratamos y deterioramos nuestras pertenencias de manera directa o voluntaria, debemos empezar a cuidar esta identidad digital porque es parte de nuestra imagen y al igual que el resto de la tecnología, nunca irá a menos y cada vez cobrará más importancia, por lo que es muy importante ser conscientes de las posibles repercusiones antes de que sea demasiado tarde.

M. H.