INFORME DE PREDICCIONES PARA EL 2017

S21SEC

Your Cybersecurity Company

ÍNDICE

26

expertos de S21sec han participado en la creación de este informe

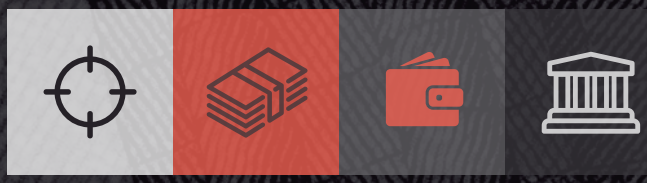
S21SEC

www.s21sec.com

1

EL USUARIO DEJARÁ DE SER EL PRINCIPAL OBJETIVO: CRECERÁN LOS ATAQUES DIRIGIDOS CONTRA ENTIDADES

EL SECTOR BANCARIO SEGUIRÁ SIENDO, INDUDABLEMENTE, BLANCO DE CIBERATAQUES.



EL SECTOR BANCARIO, UN OBJETIVO PRIORITARIO

Como hemos venido observando a lo largo de estos años, este sector es uno de los objetivos prioritarios debido a su fuerza económica. A pesar de que esta fuerza económica le permite disponer de más recursos destinados a la ciberseguridad que otros sectores, aún sigue sufriendo cuantiosas pérdidas económicas por la multitud de ciberataques que recibe. Además, hay otros motivos para comprometer la seguridad bancaria, como los ataques recurrentes por ciberterrorismo (comprometer la banca de un país significa comprometer la estabilidad del mismo) y hacktivismo. No podemos olvidar que los bancos cuentan con una gran cantidad de información sensible sobre el usuario (hábitos de compra, direcciones, etc.).

CRECEN LOS ATAQUES DIRIGIDOS CONTRA ENTIDADES

En 2017 crecerán los ataques dirigidos contra entidades. Se registrarán menos ataques a usuarios que en años anteriores, ya que actualmente la dificultad para atacar contra un usuario de un banco es mayor que en otros sectores. Creemos que crecerá el número de ataques contra la propia entidad, ya que los expertos de S21sec venimos observando esta tendencia desde los 2 últimos años. En la actualidad, hay un mayor número de APTs dirigidas contra bancos, y el malware ATM es uno de los más frecuentes. La última víctima reportada fue un banco tailandés de propiedad estatal en el que 21 cajeros automáticos fueron objeto de ataque con un botín de 350.000 dólares en efectivo para los ciberdelincuentes. Estos ataques muestran una combinación de sofisticadas técnicas de hacking, un profundo conocimiento de la estructura interna del banco y de las operaciones que se efectúan entre cajeros automáticos. Nuestra experiencia nos lleva a concluir que pueden volverse a repetir ataques como el sufrido hace pocas semanas por Tesco Bank, en el que se consiguió robar el dinero de 20.000 cuentas y con ello forzar a la filial bancaria de Tesco a suspender temporalmente todas las transacciones online. La creciente sofisticación de los ataques se hace patente cuando todavía no está claro el modus operandi utilizado para perpetrarlo.

LOS *INSIDERS*, CLAVE EN ESTE TIPO DE CIBERATAQUES

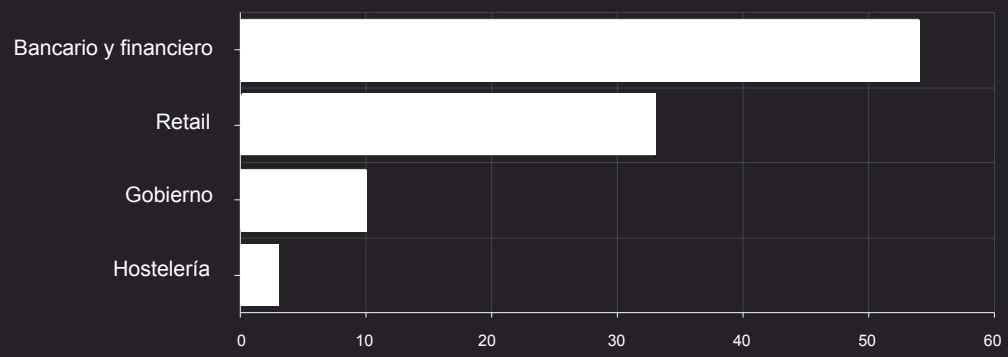
Adicionalmente, creemos que los insiders, individuos que provocan fugas de información o de datos sensibles, estarán involucrados en gran parte de estos ataques. Estos insiders podrían provenir de lugares donde el nivel de crimen organizado y corrupción es mayor y, por ello, el insider está más condicionado a agentes externos. Estos *insiders* pueden ser parte de la propia entidad o de la empresa que desarrolla el software, entre otros.

AUMENTA LA EXPOSICIÓN POR EL MODELO DE TRANSFORMACIÓN TECNOLÓGICA

El modelo de transformación tecnológica también está provocando que la banca esté mucho más expuesta a ataques a dispositivos IoT (tarjetas contactless, servicios de pago con tecnología NFC en smartphones). Además, el nivel de exposición de los bancos también es mayor por el creciente protagonismo del sector fintech (empresas que utilizan la tecnología para crear y ofrecer servicios financieros alternativos a la banca tradicional), ya que en los próximos años el sector bancario tendrá que igualar sus servicios a los de estas empresas.

LO QUE NUESTROS EXPERTOS PIENSAN SOBRE LA AFECTACIÓN DE LOS SECTORES EN 2017

De las amenazas totales que se producirán el próximo año, así es como los expertos de s21sec piensan que estarán distribuidas en cuanto a afectación por sector.



2

LOS CIBERATAQUES ESTARÁN ESPECIALMENTE DIRIGIDOS A SMARTPHONES

SE INCREMENTARÁN LOS ATAQUES DE TIPO RANSOMWARE AFECTANDO A TERMINALES MÓVILES.

TIPOS DE ATAQUE A SMARTPHONES EN 2017

Desde 2015, venimos observando el auge de este tipo de ataques por requerir de menos elaboración que otros métodos, por su rápida monetización y por el uso cada vez más extendido de smartphones. Los usuarios acabarán por infectarse con ransomware sobre todo a través de mercados secundarios, donde abundan las aplicaciones que fingen ser, sobre todo, antivirus para el dispositivo del usuario.

Tras el revuelo mundial con el Samsung Galaxy Note 7 que incluía un defecto de fábrica en las baterías que las hacía explotar, pensamos que podríamos encontrar Exploit Kits que acaben por aumentar la temperatura del móvil con el fin de dejarlo inoperativo y dañarlo, y así extorsionar al usuario. En eventos multitudinarios, donde hay una mayor competencia entre smartphones por la señal de antena, asistiremos a la implementación de antenas no legítimas para que los smartphones acaben por conectarse a la misma y pueda procederse al robo de datos que estos almacenan o a la intercepción de comunicaciones.

ANDROID VS IOS

Los ciberataques seguirán afectando en mayor medida a Android que a iOS, sobre todo a causa de las menores restricciones que existen en Android a la hora de publicar aplicaciones en la Play Store, restricciones que sí existen en la App Store. No podemos olvidar también que muchos de los pequeños dispositivos IOT también utilizan Android. Cada vez asistiremos a más ataques DDoS dada la facilidad que existe para que un determinado dispositivo forme parte de una botnet, especialmente por la falta de actualizaciones del sistema operativo, dando lugar a vulnerabilidades fácilmente explotables.

EL CONTROL DE LAS COMPAÑÍAS SE PIERDE EN LA CÚPULA DE LAS MISMAS

En cuanto al BYOD, las empresas sufrirán APTs puesto que, aunque las compañías son restrictivas en el control del teléfono, este control se pierde en la cúpula de la compañía, donde además se encuentra la información más sensible. Por ello asistiremos a ataques dirigidos contra estos dispositivos. Por ello creemos que la industria MDM (Mobile Device Management) tendrá un mayor peso a la hora de combatir APTs e invertirá en desarrollar sistemas de seguridad más avanzados.

ANDROID, EL SISTEMA OPERATIVO QUE REGISTRARÁ MÁS PROBLEMAS DE SEGURIDAD

Android será el sistema operativo que registrará más problemas de seguridad. La mayor parte de dispositivos IOT, cuya principal característica es su bajo coste (y este bajo coste repercute en la inversión en seguridad para los mismos), corren Android, por lo que en definitiva están ejecutando un kernel de Linux. Esto se da especialmente en los sensores pequeños y baratos, que a su vez son los más vendidos. Suelen conservar su contraseña por defecto, lo que facilita los ataques de fuerza bruta para acceder a los dispositivos.

ASISTIREMOS A UN MAYOR NÚMERO DE ATAQUES DDOS

Por último, cada vez asistiremos a más ataques DDoS por lo fácil que resulta que un dispositivo forme parte de una botnet: estamos rodeados de dispositivos conectados que en su mayor parte no han sido fabricados por especialistas en software, que cuentan con versiones antiguas de sistemas operativos y que rara vez lanzan actualizaciones. Esto, junto al desconocimiento de un usuario medio para detectar si sus dispositivos forman parte de una botnet, crean un escenario perfecto para que asistamos a más ataques de denegación de servicio como el que tuvo lugar en octubre de este año contra el servidor DYN y que afectó a las grandes compañías de internet (Amazon, Netflix, Twitter o Spotify, por ejemplo).

!

EN EL PRÓXIMO AÑO, SE DETECTARÁN MÁS DE 150 NUEVAS FAMILIAS DE RANSOMWARE

3

CRECERÁ EL NÚMERO DE APTS Y SE REDUCIRÁN LOS TIEMPOS DE INFECCIÓN EN INDUSTRIA

LAS INFRAESTUCTURAS CRÍTICAS SERÁN UNO DE LOS PRINCIPALES OBJETIVOS DE LOS CIBERCRIMINALES.

SE INCREMENTAN LOS ATAQUES CONTRA LA INDUSTRIA

En 2017 encontraremos un crecimiento de los ataques contra la industria, lo que la convertirá en un objetivo clave para los cibercriminales. Continuaremos siendo testigos actos de ciberespionaje y cibersabotaje a través de APTs. Estas APTs han evolucionado a lo largo de estos últimos años siendo cada vez más sofisticadas. También observaremos en este 2017 una reducción de los tiempos de infección en los sistemas. Así, se consigue reducir el rastro que se deja en ellos y se dificulta la labor de encontrar rastros de su presencia. Esto nos lleva a aventurar que es posible que en 2017 escuchemos pocas noticias sobre ataques a industria y no porque no vayan a producirse: sencillamente, resultarán casi indetectables.

Con este auge de los ataques a la industria también observaremos ataques a las herramientas y servicios que ofrecen vendedores y fabricantes para hacer frente a estas amenazas. Al mismo tiempo, se incrementarán las vulnerabilidades detectadas en equipamiento y aplicaciones de control industrial.

CONTINÚA LA PREOCUPACIÓN POR LOS ATAQUES DIRIGIDOS CONTRA INFRAESTRUCTURAS CRÍTICAS

En cuanto a las infraestructuras críticas, si bien es cierto que existe una creciente preocupación por el historial de incidentes registrados como los que tuvieron lugar en las subestaciones de distribución eléctrica ucranianas a finales de 2015, no esperamos un incremento considerable de incidentes de este tipo. Por supuesto, no descartamos que vayan a tener lugar, pero sin que haya cabida para la alarma colectiva. No obstante, la protección frente a estos ataques es crucial ya que, si bien hemos señalado que es improbable que ocurra, esto no quiere decir que sea imposible: un ataque de estas características representa una amenaza de características de tal tamaño y repercusión que una apropiada gestión del riesgo resulta clave para evitar cualquier contratiempo de seguridad.

HAY LUGAR PARA LA CALMA EN LO QUE A DAÑOS FÍSICOS SE REFIERE

Tampoco esperamos daños físicos contra personas producidos por un ciberataque: aún, por suerte, nos encontramos lejos de un escenario en el que los ciberataques trasciendan a daños físicos importantes: la dificultad de llevar a cabo de forma exitosa un ataque de estas características y de vulnerar las medidas de protección físicas en las instalaciones, que muchas veces necesitan de la acción de un individuo, siguen siendo, por suerte, un obstáculo importante para los atacantes. No asistiremos a una cantidad relevante de incidentes como el famoso suceso en una fábrica de acero alemana que tuvo lugar a principios de 2015. La tendencia será llevar a cabo ciberataques telemáticos combinados con ataques físicos a infraestructuras críticas.

AUMENTO DE LOS ATAQUES EN SANIDAD

También prevemos un aumento en el número de ciberataques en sanidad por dos motivos: primero, el robo de datos de pacientes de los amplios historiales médicos, especialmente para poder hacerse con datos de pago o información sensible que pueda servir como extorsión. Segundo, en el sector de la sanidad hay multitud de dispositivos conectados escasamente securizados. Estos ataques estarán especialmente ligados al ransomware.

Las regulaciones serán de gran ayuda para este sector, ya que obligarán a las empresas a tomar medidas que aumentarán su nivel de concienciación y seguridad. Al mismo tiempo, ya se exige a los fabricantes que los dispositivos cumplan con una serie de requerimientos de seguridad.

CONSEJOS DE LOS EXPERTOS

Históricamente, los fabricantes de equipamiento para la industria han diseñado sus aplicaciones sin tener en cuenta requisitos de seguridad. Esta tendencia cambió hace años y, aunque la situación actual ha mejorado de forma considerable, aún queda mucho camino por recorrer. Es necesaria la colaboración y asesoramiento a los fabricantes de productos para mejorar sus prestaciones en ciberseguridad. Es imprescindible continuar incluyendo en las RFPs los requisitos de seguridad derivados de un análisis de riesgos para el negocio. Las organizaciones industriales han de seguir adoptando e implantando estándares internacionales y dotando a los procesos de tecnologías enfocadas a la resiliencia y a la capacidad de recuperación frente a desastres y alteraciones en las operaciones.

También aconsejamos fomentar el trabajo entre los departamentos de IT y OT de cara a mejorar la colaboración para integrar las tecnologías de formación y operación. Una correcta gestión de riesgos requiere de un estrecho alineamiento de los encargados de gestionar las tecnologías de la información y de aquellos en carga del desarrollo final de las operaciones.

4 AUMENTARÁ LA RELEVANCIA DEL CIBERDELINCUENTE AUTÓNOMO

SIN EMBARGO,LAS BANDAS ORGANIZADAS SEGUIRÁN SIENDO MOTIVO DE ALARMA.

SE INCREMENTAN LOS ATAQUES CONTRA LA INDUSTRIA

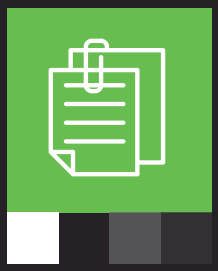
Sin lugar a dudas, las bandas de cibercrimen organizado seguirán actuando y con un papel importante a la hora de llevar a cabo con éxito sus ataques. Estas últimas semanas hemos observado, por ejemplo, cómo ha salido a la luz una banda llamada COBALT, la cual ha sido capaz de atacar los cajeros automáticos de alrededor de una docena de países europeos. Aunque estos grupos organizados necesitan de una gran inversión inicial, la sofisticación de sus ataques resulta extremadamente efectiva.

LOS MOTIVOS DEL AUGE DE LA FIGURA DEL CIBERDELINCUENTE AUTÓNOMO

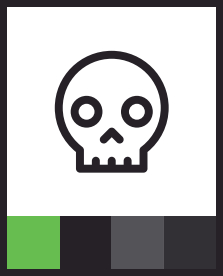
Sin embargo, esta necesidad de inversión inicial y de una infraestructura compleja hace que su puesta en marcha sea más complicada y a mayor coste. Por ello, creemos que en 2017 aumentará la relevancia del papel del ciberdelincuente autónomo, el cual no necesita de una inversión tan ambiciosa. Estos cibercriminales sin afiliación a grupos organizados utilizarán sobre todo el ransomware como forma de ataque, el cual requiere de una maniobra relativamente sencilla y con el que se consigue una rápida monetización. Estos ataques afectarán especialmente a dispositivos móviles, que serán un blanco fácil en 2017. También apostamos por el auge del Malvertising-as-a-Service, con lo que consigue monetizar el compromiso de una web sin comprometer la propia web como tal, ya que esto requiere de una mayor sofisticación en el ataque y, por lo tanto, una infraestructura y un mayor tiempo de preparación en el ataque hasta que se consigue sacar beneficio económico del mismo.

ALGUNOS DATOS PARA EL PRÓXIMO AÑO

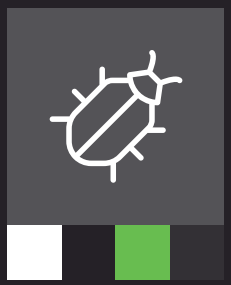
Estos son algunos datos que S21sec lanzan para el 2017 basados en las cifras recopiladas durante los últimos años y en la experiencia de nuestros expertos.



LA FORMA DE INFECCIÓN MÁS COMÚN SERÁN LOS ARCHIVOS ADJUNTOS EN CORREOS ELECTRÓNICOS, SEGUIDOS POR LOS ENLACES EN EMAILS Y DESCARGAS EN SITIOS NO LEGÍTIMOS.



EL PRÓXIMO AÑO SE DESCUBRIRÁN MÁS DE 100 MILLONES DE MUESTRAS DE MALWARE.



EN 2017, SE EXPLOTARÁN ENTRE 80 Y 100 CVES.

5

A PESAR DE LA CRECIENTE CONCIENCIACIÓN, MUCHAS EMPRESAS SEGUIRÁN TOMANDO MEDIDAS DE SEGURIDAD UNA VEZ HAYAN SIDO ATACADAS.

SOMOS PESIMISTAS EN CUANTO A LA CONCIENCIACIÓN DE LAS EMPRESAS.

SE INCREMENTAN LOS ATAQUES CONTRA LA INDUSTRIA

A pesar de que se están haciendo esfuerzos progresivamente mayores por aplicar medidas de seguridad efectivas en las compañías, especialmente por las regulaciones que se están aplicando, lo cierto es que muchas compañías siguen siendo reactivas: sólo aplican medidas para securizar sus sistemas una vez han sido atacadas o ha salido a la luz alguna noticia sobre algún ciberataque que ha afectado a la competencia. Que las amenazas dirigidas contra una compañía hagan reaccionar al resto del sector es positivo: será el cliente y el usuario final quienes acaben por disfrutar de un entorno mayor de seguridad.

Hace pocas semanas observamos esta tendencia con el ataque que afectó a Tesco Bank: los bancos británicos, tras el ataque que obligó a Tesco Bank a admitir el bloqueo de sus transacciones online y la afectación a miles de cuentas bancarias, tomaron medidas de seguridad extra para evitar posibles réplicas de ataques en sus propias infraestructuras. Esto es un comportamiento que suele darse en todos los sectores.

A PESAR DE NUESTRO PESIMISMO, OBSERVAMOS UNA CRECIENTE APUESTA POR LA SEGURIDAD

Nuestra experiencia nos hace observar una creciente apuesta de las empresas por contar con sistemas de securización. Las compañías también dedican tiempo, recursos y esfuerzos para aumentar la concienciación de sus empleados para que sean conscientes de los archivos que manejan, cómo de sensible es la información con la que trabajan y cómo deben hacer uso de la misma. La constante aparición en medios de ciberataques está provocando un efecto adverso al deseado: la falta de sensibilización al tratarse de algo cotidiano en prensa y, que por lo general no nos afecta en nuestra vida cotidiana, está conduciendo a una menor sensación de peligro en algunos usuarios. Por ello, es importante que desde las empresas se conciencie de los ciberataques sí forman parte de la realidad cotidiana y utilizar herramientas que resulten familiares para el empleado puede ayudar en este sentido.

EL RETAIL, UN EJEMPLO DE SECTOR AFECTADO POR LA FALTA DE CONCIENCIACIÓN

Un sector especialmente afectado por la falta de concienciación es el retail. En 2017 también veremos cómo el ransomware y el fraude de sistemas junto con las APTs llevadas a cabo para sustraer información se convertirán en protagonistas como amenazas para el retail. Continuarán los ataques a TPVs similares a PunkeyPos, un malware que consiguió comprometer miles de datáfonos en el año 2016 a través de un keylogger que monitorizaba las pulsaciones del teclado y de un ram-scraper, responsable de leer la memoria de los procesos que estan en ejecucion y con ello robaba los datos de las tarjetas de crédito.

Este tipo de ataques van a tener lugar tanto en las comunicaciones internas como en los proveedores externos, los cuales son en muchos casos clave en este sector. El ciclo de vida de seguridad del retail cuenta con grandes hándicaps para su protección: la seguridad de una compañía no puede ser total si sus proveedores no cuentan con medidas de protección; la cadena siempre acaba de romperse por su eslabón más débil.

El sector retail es un ejemplo de sector reactivo: hasta que una empresa no se ha visto afectada por el robo de información o por las posibles repercusiones entre sus usuarios, no toma las medidas de protección oportunas. Esto es especialmente dañino en este sector por el daño a la imagen y por las pérdidas que la caída de prestigio de una marca provoca.

CONSEJOS DE LOS EXPERTOS

Es necesario realizar una labor de concienciación con los empleados de las compañías acerca de la sensibilidad de los datos que manejan y las consecuencias de algunas de sus acciones (ser víctima de un ataque de phishing en el correo corporativo, por ejemplo). Nuestro mensaje siempre es el siguiente: la ciberseguridad comienza en uno mismo. Pero, obviamente, no podemos hacer frente a un ciberataque sólo con concienciación: necesitamos soluciones tecnológicas aplicadas como firewall, herramientas de filtrado de navegación, plataformas de protección de endpoint o herramientas de monitorización y reporting, entre otros.

www.s21sec.com