*[Informe fraude online 2008]

S21sec e-crime

*[Sobre S21sec]

S21sec, compañía española especializada en servicios de seguridad digital y líder en el sector, fue fundada en el año 2000 y cuenta con más de 265 expertos certificados. La investigación y desarrollo han constituido un objetivo prioritario en la estrategia de S21sec desde sus inicios. Esto le ha llevado a crear el primer centro de I+D+i especializado en seguridad digital de toda Europa. S21sec opera con el 90% de las entidades financieras y 26 de las grandes empresas que cotizan en el IBEX 35. Con oficinas en Barcelona, León, Madrid, Ourense, Pamplona, San Sebastián, Sevilla, Valencia, México D.F, Monterrey, Londres y Houston, S21sec ofrece servicios integrales de seguridad digital a nivel mundial las 24 horas del día.

Más información en www.s21sec.com

S21sec e-crime

ÍNDICE

S21sec e-crime

ÍNDICE GRÁFICOS

*[PRÓLOGO. S21SEC, LIDERANDO LOS ESFUERZOS CONTRA EL FRAUDE]

Las amenazas existentes hoy en día nos obligan a participar en la interminable carrera de protegernos contra todas las nuevas técnicas y tecnologías que aparecen día a día con el mero objetivo de vulnerar nuestras defensas y cometer todo tipo de delitos: fraude, robo de información, difamaciones, extorsiones, sabotajes… que no sólo nos fuerzan a poner todo nuestro empeño en proteger nuestra información a todos los niveles, sino que también muchas veces nos obliga a correr más que los demás, puesto que generalmente se cumple la máxima de que siempre se ataca al más débil.

Estos esfuerzos conllevan un conocimiento muy profundo sobre la naturaleza del problema y una experiencia contrastada del mismo; es ahí donde en S21sec se están realizando estos esfuerzos desde que comenzamos con el servicio de lucha contra el fraude a finales de 2004, y es ahí donde seguimos invirtiendo para poder luchar con éxito contra todos estos ataques.

Todos somos conscientes de que el escenario es el mismo, aunque los parámetros han cambiado, no sólo por el gran incremento del número de incidentes o la complejidad de los mismos, sino también por el grado de profesionalización de los criminales que son los responsables, y es por ello que durante 2008 hemos tenido que ir creando nuevas herramientas y servicios relacionados con la lucha contra el fraude para poder seguir siendo un referente.

Las iniciativas anteriores nos han permitido dar un gran salto cualitativo en nuestra operativa, y a la vez contribuir a la gestión de Inteligencia como pilar fundamental en el objetivo de la erradicación del fraude: perfiles de los atacantes, modus operandi, tecnologías usadas o infraestructura utilizada son, entre otros, información clave que gracias a nuestra colaboración con las Fuerzas y Cuerpos de Seguridad del Estado (FyCSE) y otros organismos y empresas internacionales (Interpol, ENISA, Microsoft, VeriSign o APWG entre otros) nos permite acercarnos cada vez más a la consecución de nuestros objetivos.

Como siempre hemos comentado, la colaboración entre todos los agentes involucrados (FyCSE, Gobierno y empresas privadas) es la clave para garantizar el éxito en la lucha contra el fraude, por tanto desde S21sec intentamos impulsar y participar en muchas de estas iniciativas, nacionales e internacionales, y de las que esperamos ver los primeros resultados durante el año 2009.

El informe de fraude online 2008 ofrece una visión totalmente objetiva de la realidad del fraude gestionado por S21sec y a la vez una radiografía clara de la evolución del mismo; y es para mí un placer poder ofrecer los resultados del trabajo realizado durante 2008 que espero que sean de su agrado y confíen en nosotros para ayudarles en la lucha contra el fraude.

Xabier Mitxelena Director General de S21sec

S21sec e-crime

*[I. INTRODUCCIÓN]

El presente informe contiene datos recogidos por los servicios de la unidad S21sec e-crime especializados en vigilancia digital, inteligencia y lucha contra el fraude en colaboración con S21sec labs, unidad de I+D+i. Este estudio ha sido realizado gracias a la colaboración de las entidades bancarias y clientes con los que trabajamos las 24 horas del día en la lucha contra los delitos en Internet. Pretende ser una radiografía de las principales amenazas en la red que actualmente afectan tanto a usuarios como a empresas. La aparición de nuevas tipologías de fraude y el aumento de la dificultad del ataque merecen un análisis pormenorizado para su conocimiento.

La colaboración conjunta entre Administraciones Públicas, Fuerzas del Orden, empresas objetivo de los ciberdelincuentes y la aportación de empresas de Seguridad de la Información como la nuestra, ha permitido trazar a lo largo de 2008 un mapa más aproximado de los focos de fraude y la identificación y detección de código malicioso, entre otras prácticas, a las que nos hemos tenido que enfrentar y que seguirán siendo un terreno de lucha en los próximos meses.

Durante el año 2008 no se han observado grandes cambios en el "modus operandi" de la mayoría de los intentos de fraude online, y seguimos agrupando los tipos de fraude en los mismos tres grandes grupos que en años anteriores: phishing, redirectores, y código malicioso. Si bien la frecuencia de estos incidentes ha sido notablemente mayor que en el año 2007, de forma global en estas tres categorías, todas las técnicas utilizadas no han sufrido grandes cambios y ello ha facilitado que los tiempos de reacción y eliminación del contenido fraudulento estén en tiempo mínimo record principalmente gracias a la experiencia acumulada de años anteriores y la innovación en las herramientas contra el fraude desarrolladas en nuestra unidad de I+D+i.

En este sentido, cabe destacar la mejora sustancial de los tiempos de cierre, pasando de cerca de 38 horas de media en enero de 2008, a 6 horas de media en diciembre de 2008, lo que constituye más de un 600% de mejora en la eficiencia.

Los incidentes recogidos corresponden a alertas producidas en el seguimiento constante de la red de este tipo de ataques. Muchos de los incidentes, afortunadamente, son erradicados en un periodo de tiempo mínimo, reduciendo la posibilidad de afectar a usuarios y entidades, pero en otros el tiempo de cierre aumenta debido a su complejidad.

Cada día los ataques son más sofisticados y provienen de expertas bandas organizadas de ciberdelincuentes por lo que se deben emplear unas herramientas de detección avanzadas y acordes a la dificultad de la amenaza. Si bien antes, este tipo de delincuencia se ejercía de manera puntual y aislada, ahora se ha convertido en una práctica generalizada, contando para ello con multitud de recursos, tanto económicos, como técnicos.

Como se ha indicado anteriormente, S21sec trabaja

conjuntamente con los equipos de seguridad de las entidades afectadas para minimizar el riesgo de los múltiples ataques detectados, así como eliminar mediante la colaboración con las Fuerzas del Or den y organismos internacionales el origen de los mismos. Para ello la formación y concienciación en seguridad se convierte en algo esencial tanto para usuarios como para el buen funcionamiento del negocio de las diferentes entidades.

Para obtener información sobre los servicios de S21sec e-crime y contra el fraude online visite nuestra página web www.s21sec.com.

El presente informe pretende ser un canal informativo para abordar el tema de los delitos en Internet desde diferentes aspectos: situación actual, principales sectores afectados, características de los ataques y medidas para la prevención y protección de los datos. Otr o año más, y siguiendo la huella del estudio anterior, hemos aportado al informe datos estadísticos recogidos desde enero de 2008 hasta diciembre del mismo año con el fin de mostrar una comparativa que muestre su evolución.

S21sec e-crime

1.1 Tipologías de fraude en internet

Desde que los primeros intentos de fraude aparecieron en Internet a finales del año 2001 en Estados Unidos, la evolución de las técnicas utilizadas ha sido paulatina, pero a la vez, constante. A finales de 2008 nos encontramos aún en la tercera fase de esta evolución (Fraude 3.0) pero con vistas a que durante el 2009 se empiece a dar el salto a la siguiente etapa.

La primera fase que tuvo lugar entre 2001 y 2005, tuvo como principal tipo de fraude el phishing; hoy en día, el phishing sigue siendo uno de los grandes peligros de Internet y constituye un problema que está aumentando rápidamente. Una de las formas más frecuentes consiste en el envío masivo de correos electrónicos, los cuales contienen enlaces que dirigen a los consumidores a webs que simulan ser la entidad real, diseñadas para capturar los datos privados del usuario: números de tarjetas de crédito, nombres de usuarios de cuentas, o contraseñas, entre otros.

Suplantando la identidad de entidades financieras, empresas de comercio electrónico, compañías de tarjetas de crédito, páginas de redes sociales, o incluso portales de la Administración Pública, los phishers consiguen convencer a los receptores para que utilicen el enlace del correo como vía de acceso a la página web fraudulenta.

La segunda fase en la evolución de las tipologías de fraude tuvo lugar entre 2005 y 2006, donde se empezaron a buscar alternativas que no necesitaran de la interactividad del usuario, e intentando utilizar infraestructuras de Internet para realizar los ataques. Una variante de este tipo de ataques es el pharming, que consiste en la redirección del usuario a las páginas web fraudulentas sin la intervención del mismo, generalmente haciendo uso de técnicas para evitar una correcta resolución de dominio mediante el protocolo DNS (el protocolo DNS es el que nos redirige a los servidores web adecuados cuando tecleamos una dirección en nuestro navegador), ya sea mediante ataques inherentes al protocolo (como la famosa vulnerabilidad aparecida en Julio de 2008 descubierta por Dan Kaminsky) o mediante el uso de código malicioso, que se comenta a continuación. Para el usuario, este ataque es totalmente transparente, ya que él introduce la dirección correcta de su entidad bancaria. Otra versión novedosa de estafa online es la práctica del vishing, a través de la cual los delincuentes consiguen los detalles de los datos bancarios de las víctimas a través de un correo electrónico o SMS que les pide que llamen supuestamente a su banco.

Por último, la tercera fase de esta evolución tiene lugar principalmente a partir de finales de 2006 hasta la actualidad, relacionada unívocamente con el crecimiento exponencial de códigos maliciosos utilizados para el fraude. Este ataque consiste en la introducción de malware (código malicioso) en los ordenadores para robar las credenciales directamente, a menudo usando técnicas cada vez más complejas. Se trata de un programa potencialmente peligroso para el usuario, generalmente no visible y que se instala en nuestro

ordenador muchas veces sin detectar nada anómalo. Estos códigos maliciosos permiten a terceras personas robar las credenciales de acceso utilizadas en Inter net, así como tomar el control total de un ordenador de forma remota, al igual que lo haría el pr opietario del mismo, por lo que es necesario seguir ciertas r ecomendaciones de seguridad para evitar este tipo de fraude.

Relacionado con el código malicioso, la mayoría de las infecciones de usuarios son debidas a la visita de una página web totalmente legítima; para ello los ciberdelincuentes añaden un pequeño código (generalmente utilizando una etiqueta iframe) en las páginas web utilizando vulnerabilidades existentes. Últimamente la forma utilizada para vulnerar estos servidor es web de forma masiva es explotando vulnerabilidades de inyección de SQL. De esta forma, se consigue introducir un código en el contenido de las bases de datos, que a la hora de presentarlo al usuario en forma de página web, intenta r edirigirle de forma automática a un servidor malicioso que trata de infectar al usuario. Existen herramientas en Inter net que permiten realizar estos ataques masivos e infectar miles de servidores web con tan sólo un click de ratón.

Una vez compr ometida la seguridad de un or denador e instalado un código malicioso en él, la amenaza principal ya no es sólo el robo de credenciales de acceso a entidades financieras, sino también el robo de todo tipo de información confidencial y sensible (documentos r eservados, correos electrónicos, información privada…), siendo esta fuga de información hacia el exterior uno de los mayores riesgos a los que se enfrentan hoy en día no sólo las empresas, sino también los gobiernos (ciberespionaje).

Como cada vez se va abriendo más el abanico de las tipologías de fraude en Inter net, es necesario contar con todos los recursos y conocimientos sobre seguridad para afrontar las posibles amenazas.

1.2 Principales sector es afectados por el fraude online

El fraude online afecta principalmente a entidades financieras, aunque también se han detectado ataques aislados a operadoras de telefonía móvil, webs de comercio electrónico, sitios de subastas, páginas bursátiles, organismos de la Administración Pública, e incluso, y cada vez más a menudo, sitios relacionados con las redes sociales, siendo esta una característica importante del próximo estadio del fraude (Fraude 4.0) donde se utilizan todos los datos r ecabados en las redes sociales para ganar credibilidad a la hora de cometer estos ataques.

A lo largo del último año, en paralelo al cr ecimiento de la banca en Internet, los ciberdelincuentes han ampliado su foco a entidades financieras de tamaño medio y pequeño, por lo que aunque los incidentes más notorios suelen asociarse a grandes corporaciones, igualmente de efectiva debe ser la lucha y la pr otección de las pequeñas y medianas empresas.

Gracias a las diferentes comisiones y grupos de trabajo tanto en España como a nivel internacional, se está generando una respuesta contundente contra estas prácticas por parte de la industria, contando cada vez con más programas educativos y herramientas técnicas que previenen, detectan y eliminan cada caso con la mayor rapidez posible.

1.3 La irrupción de las bandas organizadas en el fraude

Cada año es más patente la involucración de las bandas organizadas de crimen tradicional en la mayoría de los incidentes de fraude detectados por S21sec. Estas bandas cuentan con multitud de recursos económicos y técnicos y son los responsables de la mayoría de los delitos presentes en Internet.

Su rango de actividades es muy amplio: phishing, código malicioso, tarjetas de crédito, envío de correo no solicitado (spam), estafas (scam), venta de sustancias ilegales… utilizando para estos fines las máquinas infectadas que controlan remotamente. Muchos estudios sitúan a España dentro de los cinco países con más ordenadores infectados y desde S21sec podemos corroborar ese dato gracias a la monitorización continua que hacemos de estas redes de ordenadores infectados (botnets).

Estas bandas provienen principalmente de tres focos internacionales, aunque luego utilizan recursos por todo el mundo: Europa del Este, Brasil y Sureste Asiático. Cada uno de estos focos tiene su mercado principal y para el caso de las entidades financieras españolas, la mayoría de ataques provienen de Europa del Este pero existen conexiones entre las diferentes bandas. Asimismo, se observa una mayor presencia de amenazas provenientes del Sureste Asiático, incrementando cada año sus actividades de forma exponencial.

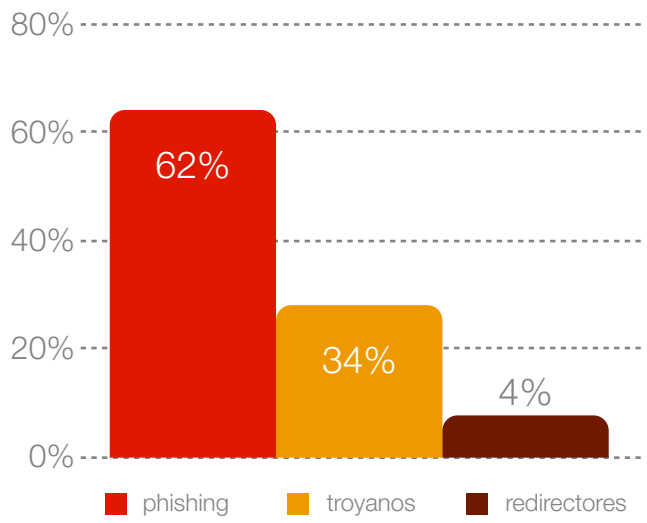
Debido a que la magnitud de las operaciones realizadas cuentan con una jerarquía bien definida, desde los dirigentes hasta las mulas, que son el último escalón, pasando por expertos programadores y administradores de sistemas y, perfectamente organizada, las técnicas que utilizan cada vez son más sofisticadas (RockPhishing, Fast-flux, Botnets, Drive-by exploits, iframe business, SEO, pump & dump, pay per install, click fraud…) para la consecución de sus objetivos, generalmente del tipo económico.

Es necesario mencionar de forma especial su mecanismo de captación de mulas, esto es, personas que aceptan recibir transacciones de dinero para luego proceder al lavado del mismo enviando ese dinero (menos un 10% en concepto de honorarios) por otro método de pago. Generalmente todos los mensajes que se reciben de cómo ganar dinero de forma rápida o como trabajar desde casa tienen como objetivo la captación de mulas. Esté atento si recibe alguno de estos mensajes y recuerde que está colaborando en la consecución de un delito de fraude si acepta colaborar en este tipo de operaciones.

2.1 Incidentes fraude online detectados por S21sec eN 2008

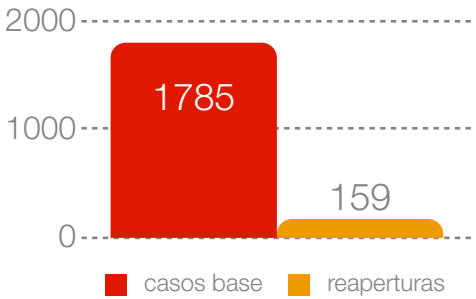
A lo largo de 2008, la unidad e-crime de S21sec detectó y solucionó un total de 3.127 incidentes de fraude en Internet dirigidos a entidades financieras en España, lo que refleja casi el doble de incidentes detectados en 2007 (1.644). Si bien el phishing continúa siendo una de las principales preocupaciones aunque desciende en relación con años anteriores -62% de los incidentes de fraude en 2008, 66% en 2007, 85% en 2006-, los ataques a través de Internet evolucionan de forma vertiginosa hacia técnicas más sofisticadas. El pasado año, la utilización de códigos maliciosos, programas que se descargan sigilosamente en el ordenador del usuario mientras navega por Internet, se han duplicado respecto a 2007 registrando un total de 1.068 incidentes. Los redirectores, técnica utilizada para dificultar el cierre de los sitios cambiando la redirección de la página de phishing de forma dinámica, han supuesto el 4% de los incidentes, una cifra poco superior al 3% registrado en 2007.

Gráfico 1. Incidentes de fraude detectados en 2008



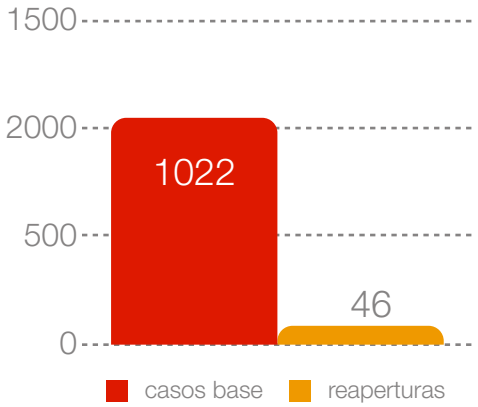
De los 3.127 incidentes detectados en 2008, 1.944 correspondían a actividades de phishing, lo que representa el 62% del total. De ellos, 1.785 correspondían a incidentes que se abrían por primera vez (incidentes base) y 159 consistieron en reaperturas de algunos de los incidentes ya existentes. Prever y hacer seguimiento de los posibles brotes (reaperturas) de un incidente constituye un aspecto esencial para garantizar los mayores niveles de seguridad.

Gráfico 2. Incidentes de phishing detectados en 2008



Los 1.068 incidentes de código malicioso detectados en 2008, se dividen entre 1.022 incidentes base, mientras que las reaperturas representan tan sólo 46 incidentes. Al igual que en los incidentes de phishing es necesario estar atento a las posibles reactivaciones para eliminar completamente la amenaza.

Gráfico 3. Incidentes de códigos maliciosos detectados en 2008



De un total de 115 incidentes de redirectores detectados, el 96% son incidentes base y tan sólo un 4% han sido reaperturas.

Gráfico 4. Incidentes de redirectores detectados en 2008

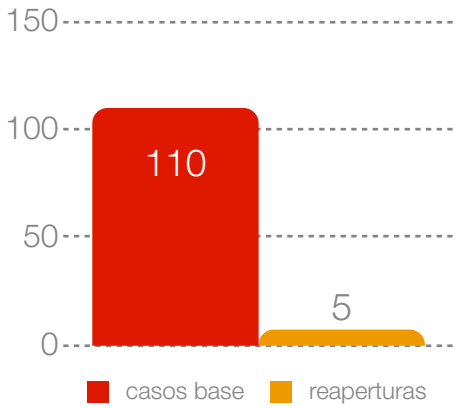
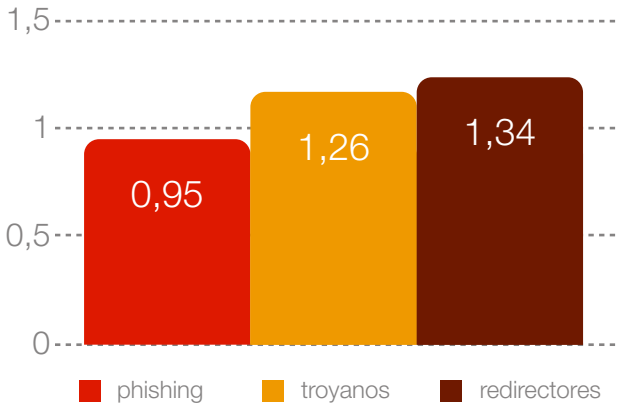


Gráfico 5. Tiempo medio cierre incidentes de phishing, código malicioso y redirectores 2008

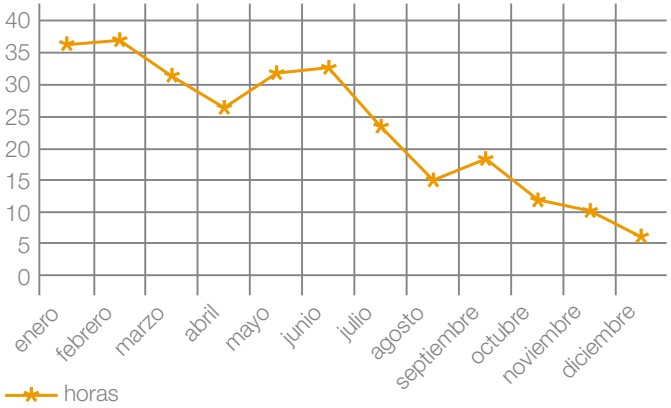


2.2 Tiempo medio de cierre en 2008

El tiempo medio de cierr e de los incidentes de fraude detectados por la compañía durante 2008 fue de 0,95 días para las acciones de phishing (frente a los 1,8 días registrados en 2007), 1,26 para los ataques mediante código malicioso (que se situaban en 3 días el pasado año) y 1,3 para los redirectores. Este tiempo denota un gran descenso con respecto a 2007 cuando, por la novedad del tipo de fraude el tiempo de cierr e se situaba en 4,5 días. Sumando las tres técnicas de fraude, el promedio de días de cierr e es de 1,2 días; se redujo 0,4 puntos respecto al pasado año que se situaba en 1,6 días.

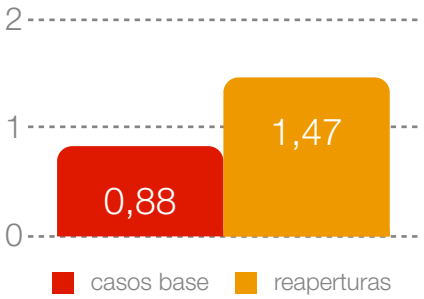
Como se ha comentado al inicio del informe, durante el año 2008 se ha conseguido mejorar de forma notable los tiempos de cierre, mejorando su eficiencia en más del 600%.

Gráfico 6. Tiempo medio mensual de cierre de incidentes



Analizando exclusivamente los incidentes de phishing, la media de tiempo empleada por la unidad S21sec e-crime fue de 0,88 para los incidentes base y de 1,47 para las reaperturas.

Gráfico 7. Tiempo medio de cierre phishing 2008



Los códigos maliciosos tienen un funcionamiento más complejo que los incidentes de phishing por lo que su tiempo de cierre resulta un poco superior, aunque ha descendido notablemente respecto a años anteriores. Los incidentes base de códigos maliciosos emplearon 1,26 días para su neutralización, mientras que para las reaperturas el tiempo promedio desciende a 1. Generalmente los incidentes relacionados con códigos maliciosos utilizan proveedores de acceso (ISP) denominados 'a prueba de balas' (bullet-proof), es decir, gestionados y protegidos por la propia banda organizada, con lo que la dificultad de cierre es mayor. Gracias a la colaboración internacional y a la red de contactos establecida por S21sec, es posible reducir el tiempo de vida de estos sitios.

Es importante reseñar la mejora en los tiempos de cierre en el transcurso de 2008 en los incidentes de phishing.

Gráfico 8. Tiempo medio mensual de cierre de los incidentes de phishing

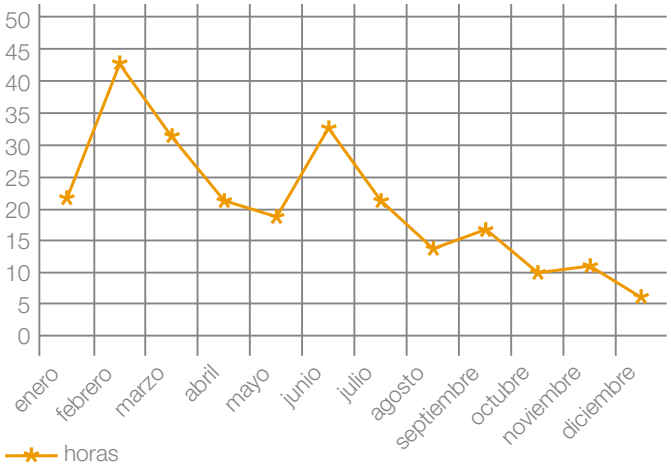
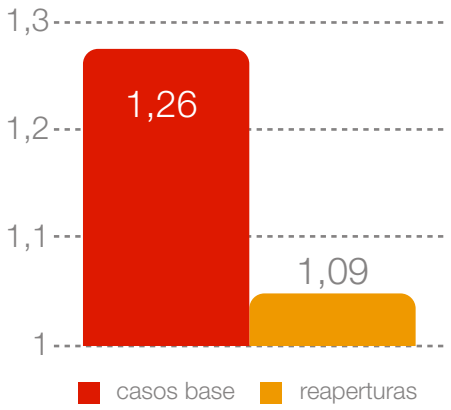


Gráfico 9. Tiempo medio de cierre de código malicioso 2008



Los redirectores han reducido sus tiempos de cierre notablemente con respecto a 2007 donde los incidentes base tenían una media de cierre de 4,5 días frente a 1,07 en 2008. En las reaperturas el descenso ha sido de casi 4 días, ya que el tiempo medio de 2007 era de 5 días frente al 0,8 de 2008.

También el descenso en los tiempos de cierre ha sido notable.

Gráfico 10. Tiempo medio mensual de cierre de los incidentes por código malicioso

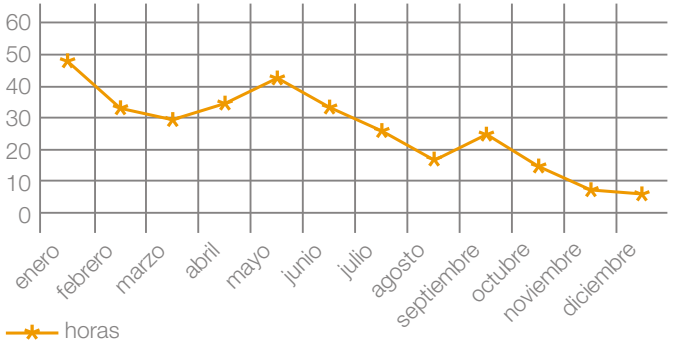
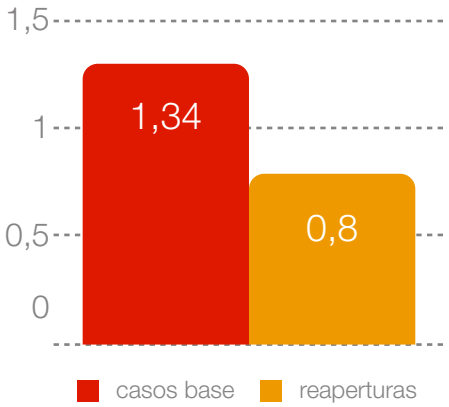
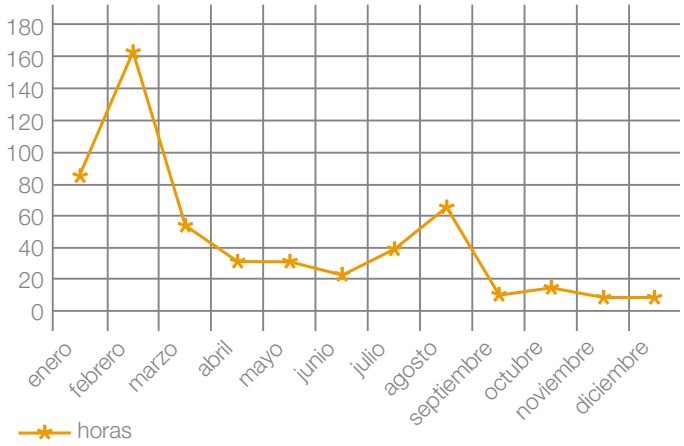


Gráfico 11. Tiempo medio de cierre de redirectores 2008



Y su evolución en tiempos de cierre.

Gráfico 12. Tiempo medio mensual de cierre de los incidentes de redirectores

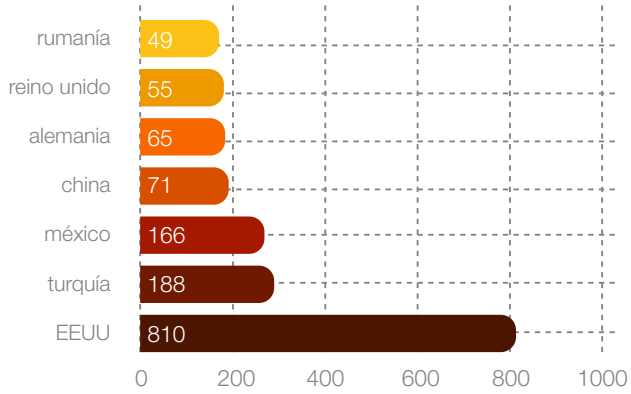


2.3 Países de alojamiento de los ataques durante 2008

2.3.1 Phishing

De los 1.944 incidentes de phishing detectados por la unidad e-crime de S21sec, 810 se alojaban en Estados Unidos, lo que supone más del 41% del total de incidentes detectados. De acuerdo a las áreas de procedencia de ataques, le siguen Turquía con 188 incidentes, México (166), China (71), Alemania (65), Reino Unido (55) y Rumanía (49). Estos datos estadísticos revelan la necesidad de colaboración con organismos y entidades de rango internacional para proceder a la detección y eliminación de los incidentes detectados. En el caso de S21sec, la colaboración con VeriSign, Melbourne IT o Microsoft son un ejemplo de la lucha conjunta en esta línea. Gracias a la experiencia acumulada en España, así como en los muchos otros países y clientes con los que los colaboradores de S21sec cuentan a nivel mundial, S21sec se posiciona como el socio más capacitado para responder a este tipo de amenazas, riesgos y vulnerabilidades.

Gráfico 13. Áreas de procedencia de los incidentes de phishing en España 2008

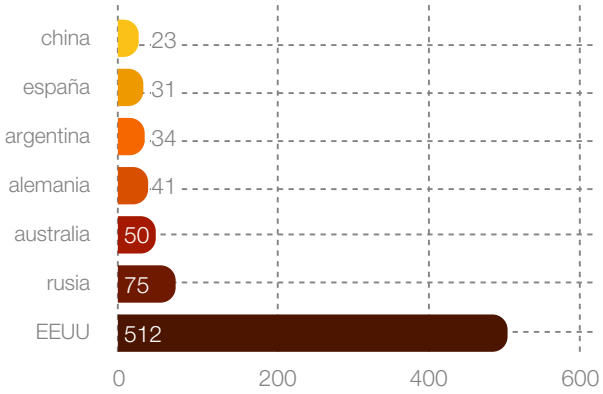


Algunos factores sociopolíticos, económicos y legales influyen poderosamente en la lucha contra el fraude online. Una legislación relajada sobre las responsabilidades de los ISP puede dificultar el proceso de cierre de un caso de phishing. La elevada concentración de ISP en un mismo país, puede tener un mismo efecto, al provocar unos beneficios marginales menores para las empresas (ISPs y registradores), haciendo que éstas inviertan menos recursos en seguridad.

2.3.2 Código malicioso

En el caso de los códigos maliciosos, los ataques con origen en Estados Unidos son los más numerosos como en años anteriores con un total de 512 incidentes, casi un 50% de la totalidad, seguidos de aquellos procedentes de Rusia con 75 incidentes (un porcentaje mucho menor ya que sólo supone el 7%).

Gráfico 14. Áreas de procedencia de los incidentes de código malicioso en España 2008

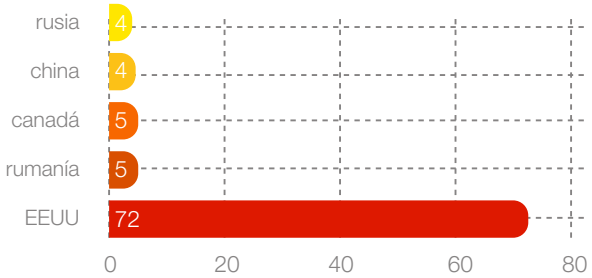


Con respecto al tiempo promedio de cierre, Islandia, Luxemburgo y Finlandia resolvieron los incidentes de forma más rápida con un tiempo inferior a 3 horas. Los incidentes más difíciles de neutralizar fueron los procedentes de Bélgica, Colombia e Israel con un promedio de 233, 160 y 224 horas respectivamente.

2.3.3 Redirectores

En el caso de los redirectores la mayor parte de los ataques proceden, al igual que en 2007, de Estados Unidos (62%); seguido de Rumanía y Canadá que sustituyen este año a Alemania y Reino Unido que ocupaban el segundo y el tercer puesto el pasado año. La respuesta más rápida de cierre se registró en los incidentes procedentes de Jamaica y Taiwán (2 horas) seguidos de Japón y Alemania tiempo de cierre de apenas 4 horas. En el extremo opuesto se sitúa el caso de Ecuador con un tiempo de clausura de 10,7 días.

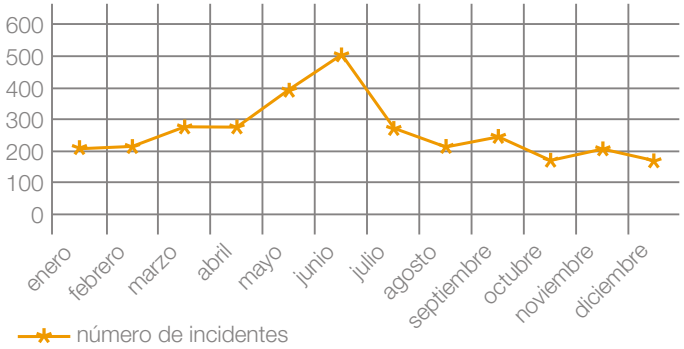
Gráfico 15. Áreas de procedencia de los incidentes de redirectores en España 2008



2.4 Evolución del número de ataques en 2008

Los incidentes de phishing, código malicioso y redirectores han tenido una evolución que se ha incr ementado progresivamente durante el primer semestr e de 2008, descendiendo en los meses finales del año. Como podemos observar, junio se convierte en el mes que más incidentes registra con un total de 504 frente a octubre que tan sólo registró 156.

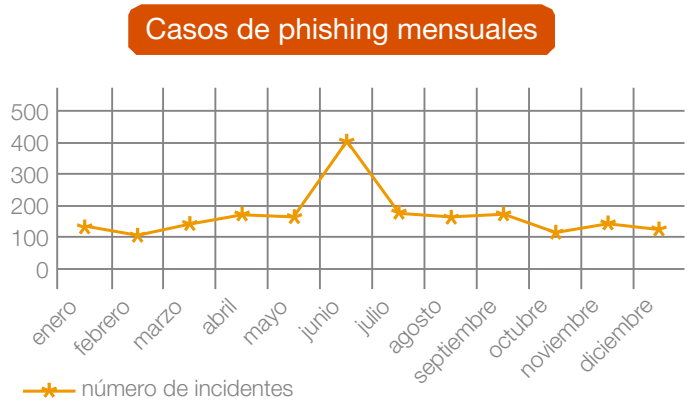
Gráfico 16. Evolución incidentes de phishing, código malicioso y redirectores por meses 2008



Durante el mes de junio, se observa un notable incremento en los ataques de phishing con 423 incidentes detectados. Comparando estos datos con los recogidos por este mismo informe sobre los ataques de phishing en junio de 2007, observamos cómo en 2008 la cifra se cuadruplica ya que hace un año los incidentes registrados eran tan sólo 106.

En el lado opuesto destaca el mes de febr ero, en el que tan sólo se detectaron 88 incidentes.

Gráfico 17. Evolución de los incidentes de phishing por meses 2008



En el primer semestre de 2008 se observa una evolución bastante homogénea durante los primer os meses. En el mes de mayo se refleja un brusco incremento, registrando 213 incidentes, que desciende vertiginosamente en junio convirtiendo a este mes en el que menos ataques ha recibido tan sólo con 84 incidentes. Diciembr e se convierte en el mes con menos incidentes de todo el año con tan sólo 45.

Gráfico 18. Evolución de los incidentes de código malicioso por meses 2008

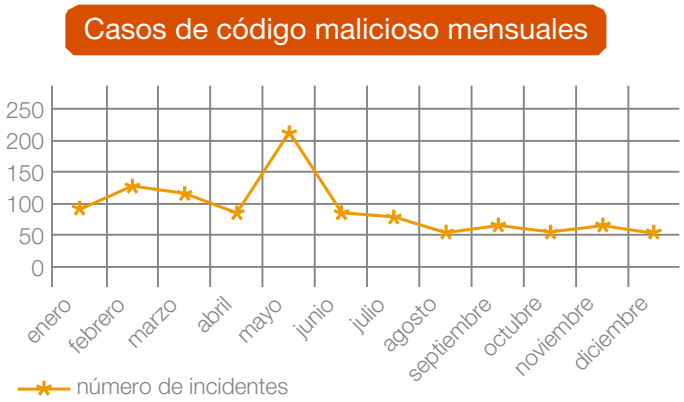
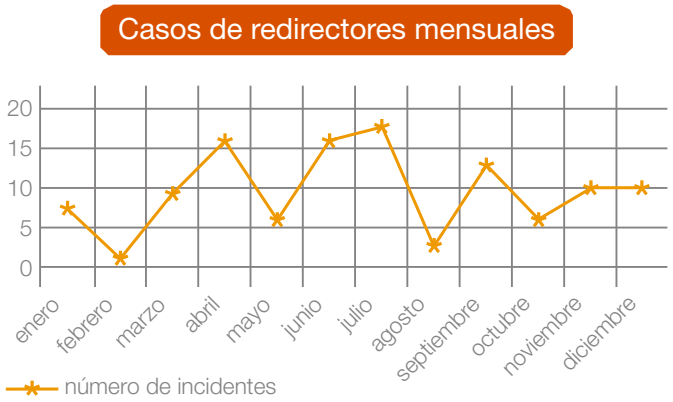


Gráfico 19. Evolución de los incidentes de redirectores por meses 2008



En el caso de los redirectores, se observa un ligero ascenso en cuanto al número de incidentes. Esto es algo normal ya que el año pasado este tipo de ataque era totalmente nuevo y se comenzaron a registrar datos a partir del mes de abril de 2007. Destaca el mes de julio con 18 incidentes y los meses de abril y junio con 16 incidentes cada uno. En el lado opuesto nos encontramos febr ero que registró tan sólo un caso.

A continuación reflejamos en unos sencillos gráficos la evolución de los distintos tipos de fraude online en los últimos años.

Gráfico 20. Total incidentes de fraude desde marzo 2005 hasta diciembre 2008

Total casos de fraude marzo 05 - diciembre 08

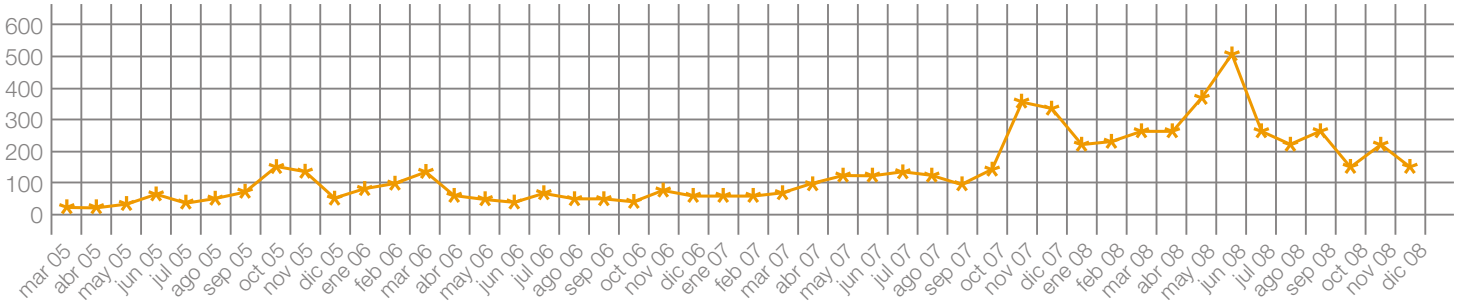


Gráfico 21. Total incidentes de phishing desde marzo 2005 hasta diciembre 2008

Total casos phishing marzo 05 - diciembre 08

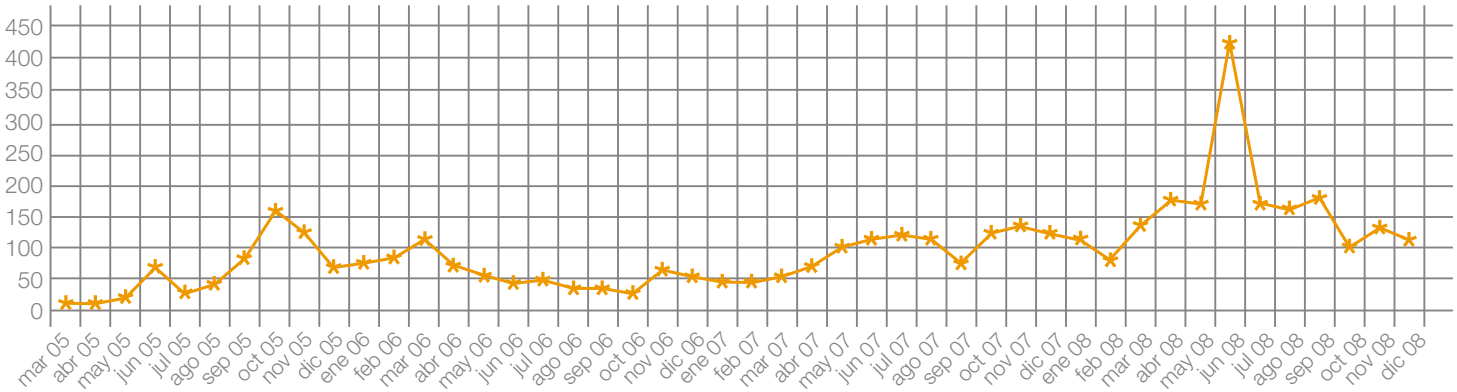


Gráfico 22. Total incidentes de código malicioso desde enero 2006 hasta diciembre 2008

Total casos código malicioso enero 06 - diciembre 08

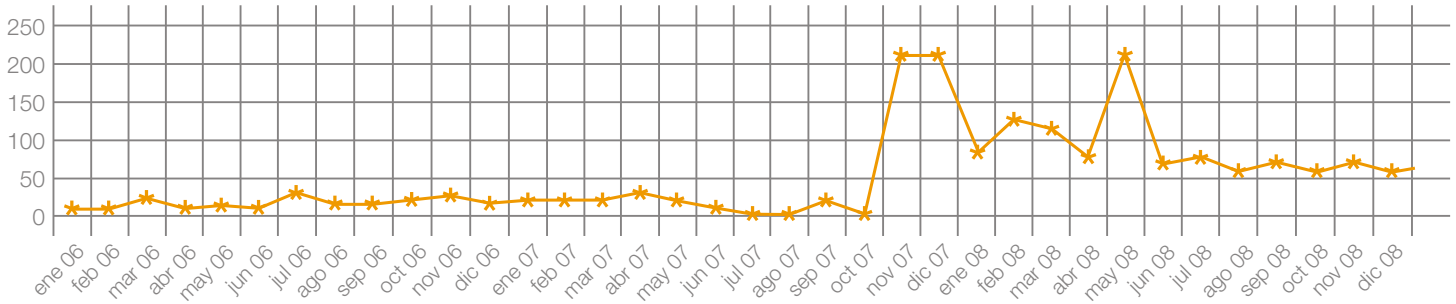
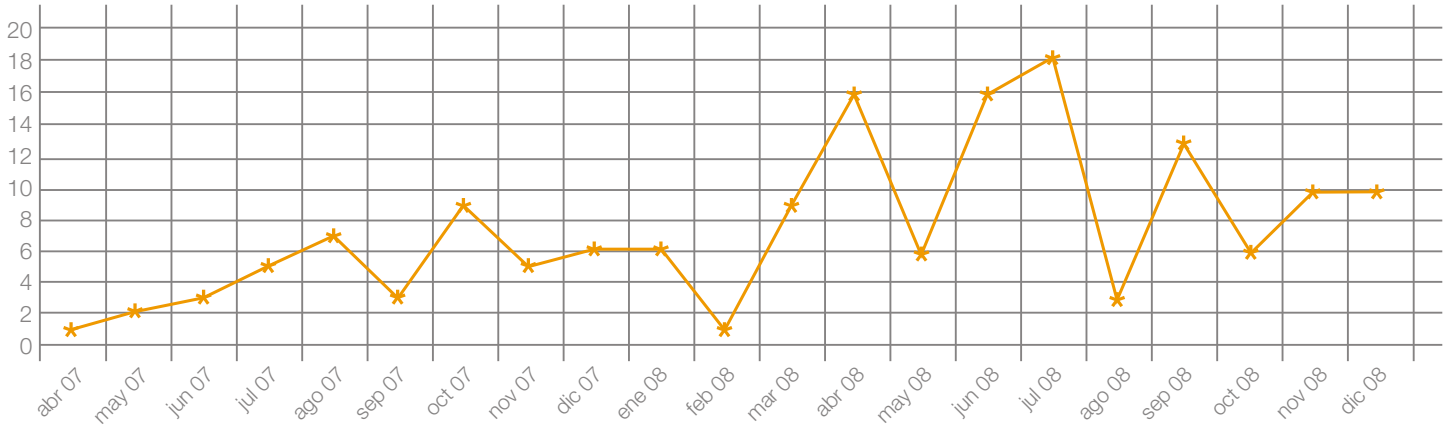


Gráfico 23. Total incidentes redirectores desde abril 2007 hasta diciembre 2008

Total casos redirectores abril 07 - diciembre 08



*[IV. TENDENCIAS Y FUTURO EN EL FRAUDE ONLINE]

Los datos presentados en este informe de fraude online demuestran el incremento de los incidentes de fraude en Internet, así como su especialización, siguiendo una evolución fuertemente marcada por el factor económico, y respaldada por la situación económica mundial.

La mayoría de las predicciones que hicimos en el anterior informe de fraude online 2007 se han ido cumpliendo e intensificando durante el año 2008: aumento del número de incidentes, complejidad del código malicioso, crecimiento de las amenazas provenientes de países emergentes, o la profesionalización de los atacantes, entre otros temas; pero también es cierto que la previsión de ver involucrados los terminales móviles en el ciclo de vida del fraude no ha experimentado un cambio sustancial.

Realmente este hecho puede ser difícil de comprender en un primer momento puesto que los terminales móviles poseen en común muchas de las características que tienen los ordenadores y que los hacen tan atractivos para ser controlados remotamente:

- Utilizan sistemas operativos
- Están conectados a la red 24x7
- Están conectados a Internet y navegan
- No se suelen seguir las recomendaciones de seguridad: no se instalan parches, no se realiza una configuración segura (hardening), no se revisan sus logs…
- Y sobre todo, los millones de terminales móviles que existen en el mundo

Gracias a la irrupción de sistemas operativos móviles donde ya es posible realizar todo tipo de actividades (navegar , gestionar el correo, mensajería instantánea…) todo apunta a que tarde o temprano veamos la proliferación de código malicioso para los principales fabricantes: Apple (iPhone), Symbian, Microsoft (Windows Mobile) y RIM (BlackBerry) puesto que ya cada vez aparecen más vulnerabilidades en estos dispositivos que pueden ser utilizadas para la instalación de código malicioso, y sobre todo que ya no es necesario basarse en el envío de SMS o MMS para poder infectar a otros terminales: ahora sólo nos hace falta modificar las decenas de tipos diferentes de infection kits que existen en Internet (Mpack, FirePack, IcePack, Gpack, AdPack…) para que soporten exploits para estos dispositivos.

Otra de las predicciones que se va a intensificar durante 2009 es el abuso de datos personales no sólo para poder enviar mensajes de correo personalizados que intenten atrapar al receptor, sino para utilizar esos datos en intentos de fraude directo debido al gran conocimiento que tenemos de la persona. Es tan simple como conseguir acceso al perfil de una persona en una red social (FaceBook, Tuenti…) y hacerse pasar por algún familiar o amigo en apuro en alguna ciudad extranjera que necesita dinero para comprar un billete de avión puesto que le han robado todo su dinero.

Las redes sociales van a jugar un papel fundamental en las siguientes fases de la evolución del fraude y a día de hoy no está muy clara cuál es la mejor alternativa para protegerse de cualquier intento de ataque: usurpaciones de identidad,

difamaciones, publicación de información privada o confidencial, gusanos…

Por otro lado, con el recrudecimiento de la situación económica mundial, cada vez existirán más intentos de fraude tradicional (recepción de dinero, premios de lotería, regalos gratuitos inexistentes que hay que pagar los gastos de envío…) y por supuesto, fraude relacionado con las entidades financieras (phishing, pharming y código malicioso), captación de mulas, etc. y otras entidades gubernamentales, siendo un claro ejemplo la campaña de la Declaración de la Renta, donde es posible que utilice como pretexto la devolución de dinero para cometer fraude por parte de criminales.

A finales de 2008 la aparición de Conficker hizo replantearse la falsa sensación de seguridad que muchas veces tienen las organizaciones, y siendo el hombre el único animal que tropieza dos veces en la misma piedra, es muy probable que en los próximos años vivamos situaciones parecidas donde se aprovechan gusanos como el Conficker como una pieza fundamental en la infraestructura del fraude, ya sea como elemento de propagación de código malicioso, envío de spam, o actividades más dañinas como el robo de información y cualquier intento de extorsión.

Finalmente, desde el punto de vista técnico, la complejidad de los ataques va a seguir evolucionando de forma natural, sobre todo debido a la utilización de todas las tecnologías presentes en Internet (P2P, proxies inversos, redes VPN, fast-flux, intercambio de rutas BGP, SEO y banners de publicidad maliciosos…) que dificultarán la detección y la respuesta ante cualquier tipo de incidente relacionado con el fraude.

*[V. DECÁLOGO DE MEDIDAS CONTRA EL FRAUDE ONLINE]

5.1 Consejos para las organizaciones

1. Sea consciente de que la seguridad es un aspecto crítico para su negocio. En nuestros días, el valor fundamental de una compañía son los activos intangibles. Un fallo en el funcionamiento de los sistemas informáticos de la compañía o una pérdida o robo de información pueden suponer un tiempo de inactividad –con las consiguientes pér didas económicas- o, incluso, la desaparición para un negocio. Además, en determinados sectores, como la banca y el comercio electrónico, es necesario generar confianza en los consumidores y usuarios actuales y potenciales, y sólo un adecuado nivel de seguridad garantiza la cr edibilidad del negocio.

2. Cuente los recursos destinados a proteger la seguridad de sus sistemas de información como una inversión, no como un gasto. Se trata de mantener la seguridad de un aspecto crítico para su negocio. Por tanto, debe abordarlo como un aspecto global, que debe impregnar todas y cada una de las rutinas y pr ocesos que tengan lugar en la organización.

3. Conozca sus debilidades. Encargue a pr ofesionales especializados un estudio de vulnerabilidades de sus sistemas de información, para conocer en detalle los riesgos a los que está expuesta su organización, tanto exter nos (atacantes, código malicioso…) como internos (mal uso de la información por parte de empleados o acceso de éstos a información confidencial).

4. Actualice el softwar e, antivirus y cortafuegos de su empresa. Aunque no es suficiente para alcanzar un grado óptimo de seguridad, mantener al día los pr ogramas informáticos con parches de seguridad y actualizaciones, antivirus y cortafuegos de la empresa ayudará a mantener a raya a virus, troyanos y otros tipos de código malicioso.

5. Vigile los accesos y el tráfico de información de sus sistemas informáticos. Hoy día, los pr ofesionales especializados pueden monitorizar permanentemente las entradas y salidas a los sistemas de información de una organización y todo el tráfico que se produce dentro de los mismos. Relacionando todos esos datos entre sí, se pueden detectar intentos de acceso fraudulento o extracciones anómalas de información y comprobar si efectivamente se trata de un intento de delito, lo que permite, en caso de que así sea, tomar las medidas oportunas.

6. Manténgase atento a los movimientos sospechosos que puedan producirse en su entorno. Los servicios de vigilancia digital permiten detectar el r egistro de dominios o sitios web que intenten suplantar el nombre de la organización, copiar su home o utilizar fraudulentamente su marca. Atajar estos movimientos a tiempo puede evitar que la organización sea víctima de un futuro fraude o vea seriamente dañada su credibilidad.

7. Establezca una política clara de acceso a la información. Ya sea a través de un sistema de claves o de cualquier otro, defina claramente quién puede acceder a cada información

y en qué condiciones. De esta forma, podrá controlar mejor la seguridad de sus activos digitales.

8. Ponga en marcha un plan de formación interna en materia de seguridad. Todos los miembros de la organización, así como clientes, proveedores y todo aquel que tenga acceso a los sistemas de información deben recibir formación en materia de seguridad e implicarse en la tarea de mantenerla, desde el director general hasta el último trabajador.

9. Deje la seguridad de la organización en manos de profesionales. Sólo los expertos podrán analizar sus necesidades y ofrecerle lo que más le conviene, protegiendo sus sistemas de información y liberando al personal interno de esa tarea.

10. Instaure una verdadera cultura de la seguridad en su organización. Implíquese, implique a todos los miembros de su equipo, trate la seguridad como un aspecto estratégico para su negocio y déjela en manos de expertos. Si, a pesar de todo, su empresa es víctima de un delito, póngalo en conocimiento de los profesionales y de las autoridades y ellos actuarán para minimizar en lo posible el impacto de ese ataque.

5.2 Consejos para los particulares

1. Acceda siempre a la web de su banco o a los portales de comercio electrónico desde un ordenador de su confianza. No realice transacciones electrónicas, en especial aquellas que impliquen la introducción de claves privadas, a través de un ordenador de uso público.

2. Mantenga el navegador, lector de ficheros .pdf, antivirus… actualizados y con los últimos parches de seguridad instalados. De esta forma, estará más protegido ante cualquier código malicioso que busca introducirse en su ordenador para capturar las claves cuando usted las introduce.

3. Manténgase informado de las últimas novedades en materia de seguridad informática. Lea también las recomendaciones y avisos de seguridad que su banco o caja pública a través de su web.

4. No facilite nunca sus claves personales a terceros por teléfono, fax o por correo electrónico. Su banco nunca le contactará por estas vías para pedirle este tipo de información.

5. Desconfíe de los correos electrónicos que le soliciten sus claves con urgencia. Suelen utilizar argumentos como la detección de un posible fraude, problemas técnicos o concursos, y amenazan con cerrar o bloquear su cuenta si no envía sus claves por correo o las introduce en una web a la que se accede a través de un enlace adjunto. Si sospecha, contacte directamente con su banco o caja.

6. Acceda a su banco o a los portales de comercio electrónico tecleando siempre la dirección URL en el navegador. No acceda a estos sitios web a través de enlaces

proporcionados por terceros: pueden conducirle a una copia de la web auténtica creada para capturar sus claves.

7. Cuando se disponga a realizar transacciones electrónicas, asegúrese de que la web utiliza un protocolo seguro. Esto puede comprobarse fácilmente observando si la URL comienza por https://, donde la "s" indica que se trata de un sitio seguro. También debe aparecer un candado en la parte inferior derecha de la pantalla. Dado que algunos delincuentes falsifican este símbolo, es conveniente comprobar su autenticidad haciendo doble clic sobre él: de esta forma, aparecerá la autoridad certificadora de la seguridad del sitio.

8. Compruebe regularmente los movimientos de su cuenta bancaria. De esta forma podrá saber si se ha producido alguna transacción que usted no ha ordenado y actuar en consecuencia.

9. Si en algún momento sospecha que se encuentra ante un caso de phishing, o que usted ha sido víctima de un delito de este tipo, contacte con su entidad bancaria. Ellos se encargarán de minimizar el impacto del ataque y de tomar las medidas oportunas para atajar el ataque a tiempo.

10. Actúe en todo momento con sentido común: sea cauto. Ante la más mínima sospecha, contacte con su proveedor de servicios financieros. Ellos resolverán sus dudas.

5.3 Decálogo de protección contra fugas de información

1. Definir los niveles de clasificación de la información dentro de una empresa (sensible, confidencial, top secret...) y aplicar estos niveles a toda información ya sea digital o en papel.

2. Establecer en la política de seguridad de la empresa buenas prácticas relacionadas (tiempo para acceder a lo impreso, mesas limpias de documentos, destrucción de información importante (papel, copias de seguridad, etc.).

3. Acceder a la información importante sólo desde dispositivos y redes autorizadas (evitar ciber cafés, ordenadores de casa, redes públicas wireless, etc.).

4. Utilizar el "need to know", es decir, evitar el acceso a la información si realmente no existe una necesidad.

5. Monitorizar el acceso y uso de la información importante (herramientas de gestión de logs y herramientas DLP: Data Loss Prevention).

6. Monitorizar la información que existe en Internet sobre la organización.

7. Establecer sesiones de formación dentro de la organización para los empleados en temas de concienciación, test anuales (ingeniería social, clasificación de la información...).

8. Conocer las últimas técnicas utilizadas en delitos de ciberespionaje o conseguir un asesoramiento por parte de empresas especializadas.

9. Establecer capas de seguridad a todos los niveles (perímetro, puesto de usuario, salida...) para evitar posibles intrusiones tanto externas como internas.

10. Realizar test de intrusión tanto externos como internos para conocer los riesgos existentes.

Colabore en la prevención del fraude online, su participación es importante. Si detecta posibles correos fraudulentos contacte con nuestro servicio de alerta en el correo antiphishing @ s21sec.com o a través de nuestra web www.s21sec.com

*[Pamplona . San Sebastián . Barcelona . Madrid . Ourense . León
Sevilla . Valencia . México DF . Monterr ey . Londres . Houston]

S21sec e-crime