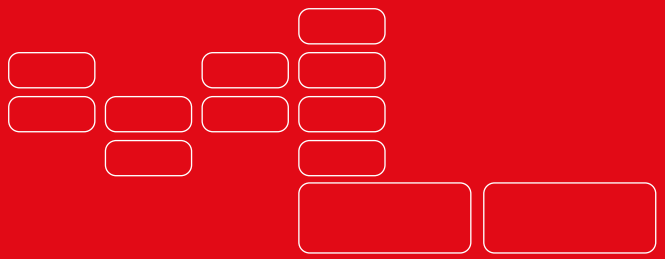
Informe anual de Fraude Online y Cibercrimen 2010

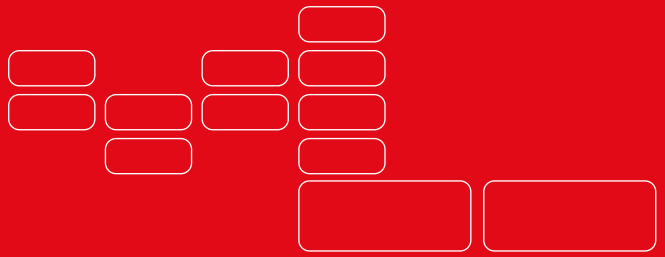


S21sec e-crime

Índice

Índice de gráficos

Prólogo



Prólogo

Un año más presentamos el informe de fraude anual, con el principal objetivo de describir el estado del fraude por Internet (third party fraud o fraude en tercera persona) durante el año 2010. Como en los anteriores informes, en él se describen diferentes características de los incidentes a los que S21sec ha respondido, en colaboración con todos los afectados, proveedores de acceso, registradores, policías y CERTs de todo el mundo.

Si comparamos la cifra total de incidentes en 2010 respecto a años anteriores, podemos ver que realmente ha habido un crecimiento vertiginoso de los casos de fraude por Internet, casi duplicando la cantidad, hasta llegar a 5.337, lo que denota principalmente que cada vez hay más actores detrás de estos ataques, aunque las técnicas utilizadas son casi idénticas a lo que hemos estado viendo durante estos últimos años.

El phishing sigue siendo una técnica ampliamente utilizada por los atacantes, técnica que se caracteriza por su simplicidad y su bajo coste de puesta en producción (al fin y al cabo, es un ataque de ingeniería social), y que durante 2010 supuso el 60% de los ataques. Como característica nueva, ya no son solamente entidades financieras las afectadas, sino que cualquier motivo es válido para intentar engañar al usuario pidiéndole información particular: empresas de telefonía, de transportes, gubernamentales o incluso marcas famosas son utilizadas por los criminales como gancho para pedirnos nuestros datos personales y de tarjetas de débito o crédito. Si bien las entidades financieras han desplegado casi en su totalidad las tarjetas con el estándar EMV para evitar fraudes que principalmente venían del clonado de tarjetas, hoy en día aún se sigue utilizando la banda magnética en muchos establecimientos o la comprobación de los datos utilizados en las compras por Internet. Por lo tanto, aunque de forma paulatina se está haciendo la vida más difícil a los atacantes para rentabilizar los datos relacionados con tarjetas, aún es pronto para poder decir que no tienen nada que hacer. En el caso de los accesos a la banca online, el phishing tiene cada vez más problemas para conseguir sus objetivos, puesto que prácticamente la totalidad de las entidades financieras han implementado medidas de seguridad que obliga al atacante a tener que conseguir más información o controlar al usuario para poder realizar las transferencias (segundo factor de autenticación, PINsentry, autenticación por SMS, etc.).

En el caso del código malicioso, que supone un 32% de los incidentes detectados, sí que se ha observado una evolución con respecto al año anterior. Quizás no una evolución en la técnica empleada para intentar cometer el fraude, pero sí que se han visto nuevas familias de código malicioso, así como nuevas plataformas para la infección acordes al uso de la tecnología actual.

A la hora de intentar robar las credenciales de un usuario, en Europa, EEUU y Australia la inyección de código sigue siendo la práctica más habitual, aunque gradualmente se ha ido migrando al uso de javascript de forma más intensiva para realizar estas inyecciones, con el principal objetivo de poder realizar los famosos y temidos ataques 'man-in-the-browser' de forma totalmente transparente para el usuario (con todas las ventajas y problemas que tiene el uso de javascript). En cambio, en Latinoamérica se sigue apostando por códigos maliciosos que simulan el navegador o la aplicación bancaria para robar las credenciales; esto es, son mucho más sencillos, no interfieren con el navegador, pero su finalidad y casi su grado de éxito son parecidos.

También durante 2010 hemos visto nuevas familias de código malicioso que probablemente vienen a sustituir a familias ya veteranas como ZeuS. Durante el segundo semestre de 2010 los incidentes relacionados con SpyEye han ido creciendo de forma bastante rápida, así como otras familias como Carberp. Son códigos maliciosos que ya parten de un caso de éxito (ZeuS), e intentan solucionar todos los problemas y errores que ha tenido éste. Todavía su uso no es tan generalizado, pero ha sido durante 2010 cuando se han empezado a usar de forma más habitual.

Pero la característica más importante que hemos visto en 2010 referente al código malicioso ha sido el salto a una nueva plataforma: los móviles. Siempre hemos comentado que los móviles tarde o temprano serían objetivo de los criminales, pero hasta este año no ha habido ningún caso realmente vinculado con el crimen económico y, como no, relacionado con la familia de ZeuS. La razón de este nuevo objetivo es clara: cada vez se utiliza más el móvil para acceder a la banca online, incluso para autenticar transacciones financieras (ya sea mediante una aplicación o un SMS), y la forma más sencilla para poder controlar este nuevo dispositivo es infectarlo. Así pues, una vez que una computadora es infectada por ZeuS, también se pide el número y modelo del teléfono móvil para enviarle por SMS un enlace para la descarga e instalación de un supuesto certificado de seguridad. Este 'certificado de seguridad' intercepta todos los SMS recibidos para enviarlos silenciosamente al número que deseáramos. De esta manera, es totalmente trivial obtener los SMS de autenticación que envían algunas entidades financieras para la seguridad de una transferencia.

Las plataformas que hemos visto relacionadas con esta nueva técnica son BlackBerry, Symbian y Windows Mobile, aunque también a lo largo del año han ido apareciendo cada vez más código malicioso para plataformas Android (y de iOS ya recordamos el gusano iKee que tenía un cierto componente económico). En definitiva, claramente ya los dispositivos móviles (tablets, teléfonos) son una plataforma muy atractiva para el control por parte de terceros (no sólo para el robo de información, sino para los mismos objetivos que tenían las computadoras, como realizar DDoS, utilizarse como proxy, albergar archivos, etc.)

En resumen, el año 2010 ha sido un año muy intenso en lo que a fraude se refiere, no sólo por el crecimiento en el número de incidentes, sino también por la aparición de nuevas técnicas y familias de código malicioso que obligan a tener que estar continuamente trabajando en herramientas y servicios para evitar todos estos nuevos ataques. Si bien ha sido quizás el año donde hemos tenido que esforzarnos más, también ha sido en el que más hemos aprendido y hemos podido utilizar todo nuestro conocimiento para evolucionar y adaptarnos a las nuevas amenazas. Cada vez son más clientes los que confían en S21sec para protegerse contra estas amenazas, y es para nosotros una enorme responsabilidad estar a la altura y poder reaccionar con garantías de éxito contra todos los atacantes.

Espero que la lectura del informe sea de su agrado, y no dude en contactar con nosotros para cualquier consulta.

David Barroso
Director S21sec e-crime

Introducción

Introducción

El pasado año 2010 no pasará a la historia por haber sido un año de innovaciones en cuanto a la concepción y la arquitectura del fraude en Internet se refiere, pero es posible que se haya puesto la primera piedra para años venideros. En términos generales se ha continuado la senda de especialización del fraude comenzada en años anteriores, teniendo como gran protagonista nuestro viejo conocido troyano ZeuS, y como nueva estrella del espectáculo a SpyEye.

Prácticamente desde su aparición en 2007 ZeuS ha sido el troyano predominante en el fraude bancario en Internet, y el pasado año 2010 no podía ser menos.

Durante este periodo hemos podido observar cómo se han combinado a la perfección el uso de viejas técnicas como *"fast-flux"* o *"bulletproof hosting/registrar"* con las nuevas tendencias en Internet, las redes sociales: Twitter, Facebook, Tuenti, todas ellas han sido utilizadas como vector de entrada y difusión para lograr el mayor número de infecciones posibles.

Además hemos sido testigos del poder de adaptación al medio de estos troyanos, que han sabido evolucionar a cada una de las barreras implementadas por las entidades bancarias. Hemos comprobado la solución de ZeuS para atacar el segundo factor de autenticación, "Man in the Mobile" (MitMo).

Mediante el uso de ingeniería social se lograba infectar el teléfono móvil del cliente, teniendo la capacidad de manipular los envíos de contraseñas OTP enviadas para la realización de transacciones.

De manera similar SpyEye era capaz de sortear con éxito otra de las barreras, el uso de sistemas expertos de detección de fraude mediante el uso de la técnica conocida como "Man in the Browser" (Mitb). Conceptualmente la idea es sumamente sencilla, el propio usuario debe realizar la transacción en una sesión valida. El troyano una vez detecta que el usuario está en una sesión válida, realiza una petición a un servidor externo, que en función del capital de la cuenta, suministra un destinatario de la transferencia (mula) y realiza la transferencia en segundo plano. En primer plano, el usuario no es consciente de ninguna operación ya que el troyano controla la capa de presentación del navegador y oculta el movimiento del capital.

Ambos casos de éxito de la evolución de un troyano bancario fueron descubiertos por S21sec, que aportó medidas para la solución de dichas incidencias. Sin embargo la mayor evolución que se ha producido durante el pasado año se ha dado lugar en la afectación de estos riesgos. Durante los últimos años hemos tenido prácticamente en exclusiva a las entidades bancarias como objetivos del fraude, sin embargo ahora el "mercado" se ha ampliado. Cualquier empresa en la que sea posible la monetización del fraude es ahora objetivo de los ataques: empresas que proporcionan servicios de pago electrónico, pasarelas de pago, sector turístico y tiendas de comercio electrónico.

En resumen, durante 2010 los ciberdelincuentes han sido capaces por una parte de especializar aun más los ataques por Internet, y por otra parte ampliar el rango de empresas objetivo de los mismos obteniendo un mayor margen de beneficios de todas las actividades relacionadas con el fraude en Internet.

Datos estadísticos

Datos estadísticos de 2010

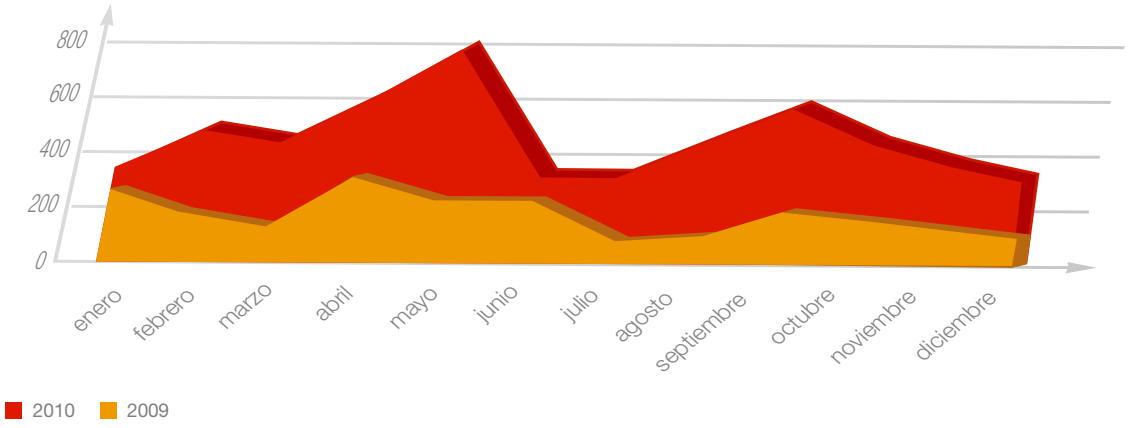
Casos fraude online detectados por S21sec en 2010

Durante el año 2010, **S21sec e-crime** detectó y solucionó un total de 5.337 casos de fraude en Internet dirigidos a entidades financieras en España, lo que refleja más del doble de casos detectados que en 2009 (2.534).

El phishing, que constituye más de un 60% de los casos, continúa siendo la principal preocupación a pesar de que se ha mantenido en niveles inferiores a los registrados el año pasado (64%) en una tendencia claramente descendente marcada durante los últimos estudios.

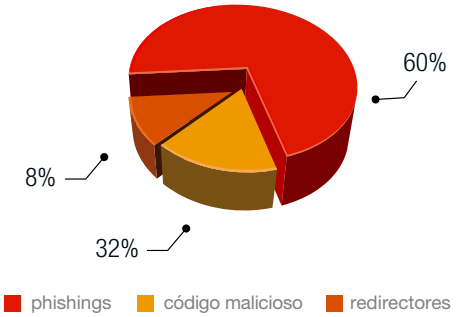
No obstante, la precisión y meticulosidad de los ataques a través de la Web no han dejado de evolucionar rápidamente mediante técnicas más avanzadas y peligrosas. Buena prueba de ello es que el pasado año la utilización de códigos maliciosos, también se duplicó respecto a 2009, registrando un total de 1.705 casos frente a los 750 anteriores. Por su parte, los redirectores han supuesto el 8% de los casos, una cifra muy similar al 7% registrado en 2009.

Gráfico 1: Evolución casos de fraude.



> *De este modo, de los 5.337 casos detectados en 2010, 3.191 correspondían a actividades de phishing, lo que representa el 60% del total.*

Gráfico 2: Casos de fraude detectados en 2010.



De ellos, 2.849 correspondían a casos que se abrían por primera vez (casos base) y 342 consistieron en reaperturas de algunos de los casos ya existentes (ver gráfico 3).

Por su parte, los 1.705 casos de código malicioso detectados en 2010 se dividen entre 1.529 casos base, mientras que las reaperturas representan tan sólo 176 casos. Al igual que en los casos de phishing, es necesario estar atento a las posibles reactivaciones para eliminar completamente la amenaza.

En tercer y último lugar, de un total de 441 casos de redirectores detectados, el 83% son casos base y tan sólo el 17% han sido reaperturas.

Gráfico 3: Casos de phishing detectados en 2010.

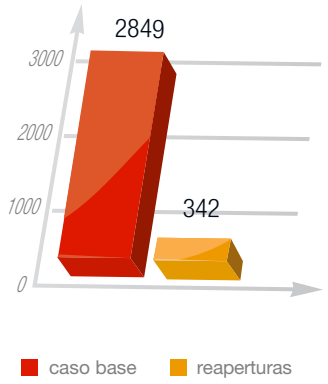


Gráfico 4: Casos de código malicioso detectados en 2010.

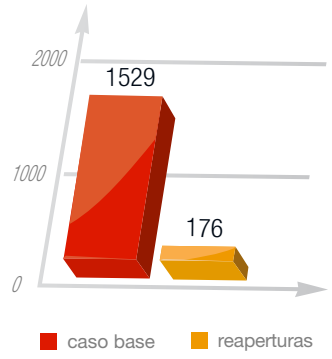
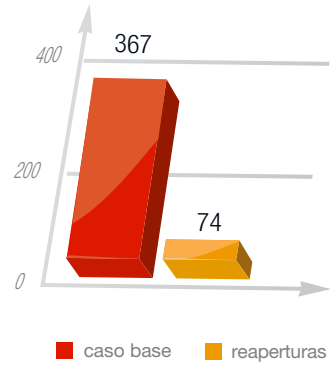


Gráfico 5: Casos de redirectores detectados en 2010.



> *"No hay que olvidar que anticiparse a la amenaza y hacer un seguimiento estricto de los posibles brotes (reaperturas) de un caso constituye un aspecto esencial para garantizar los mayores niveles de seguridad."*

Tiempo medio de cierre en 2010

El tiempo medio de cierre de los casos de fraude detectados por la compañía durante 2010 fue de 1,18 días para las acciones de phishing, junto con un intervalo de 2,74 días para los ataques mediante código malicioso y 1,31 días para solventar los redirectores.

A modo general y teniendo en cuenta los tres tipos de incidente, el promedio de días de cierre se coloca en 1,74 días, una cifra algo superior a la registrada en años anteriores.

Por otro lado, si se analizan exclusivamente los casos de phishing, la media de tiempo empleada por S21sec fue de 1,15 para los casos base y un cercano 1,21 para las reaperturas.

Paralelamente, los códigos maliciosos, por su complejidad, requieren un sistema más laborioso de cierre. Así, los casos base de códigos maliciosos durante 2010 emplearon 2,19 días para su neutralización.

Gráfico 6: Tiempo medio cierre casos de phishing, código malicioso y redirectores 2010.

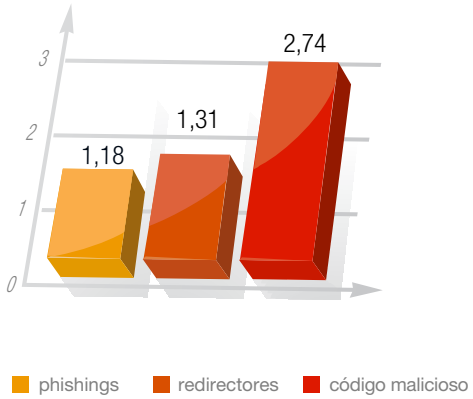
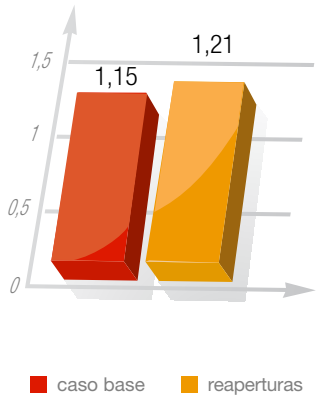


Gráfico 7: Tiempo medio de cierre phishing 2010.



Generalmente los casos relacionados con códigos maliciosos utilizan proveedores de acceso (ISP) denominados 'a prueba de balas', es decir, gestionados y protegidos por la propia banda organizada encargada de realizar el ataque, y por este motivo la dificultad de cierre es siempre mayor. No obstante, gracias a la colaboración internacional y a la red de contactos establecida por S21sec, es posible seguir reduciendo el tiempo de vida de estos sitios.

Los redirectores han reducido sus tiempos de cierre con respecto a 2009 donde los casos base tenían una media de cierre ligeramente superior, con un valor de 1,58 días para la anulación de casos base, y de 1,05 días para finalizar los casos de reaperturas. Como se puede observar a continuación, los baremos de estas categorías son más afines a los registrados en los ataques de phishing.

Gráfico 8: Tiempo medio de cierre de código malicioso 2010.

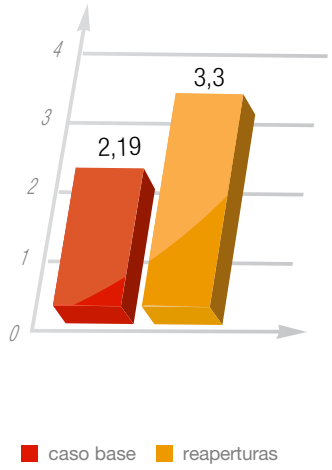
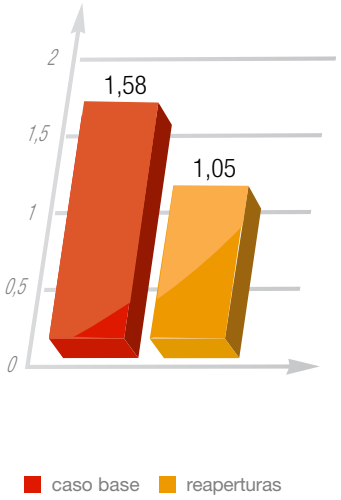


Gráfico 9: Tiempo medio de cierre de redirectores 2010.



Países de alojamiento de los ataques durante 2010

En este punto pasaremos a detallar cuáles son los principales países de procedencia de los ataques de fraude online por tipología.

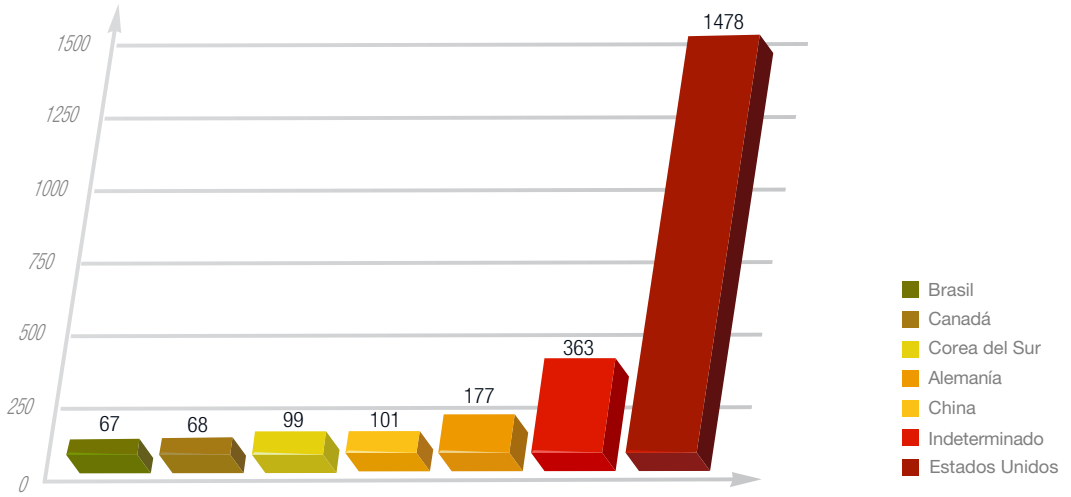
Phishing

De los 3.191 casos de phishing detectados por S21sec e-crime , 1.478 se alojaban en Estados Unidos, lo que supone más del 46% del total de casos detectados. De acuerdo a los países de procedencia de ataques, le siguen los que no revelaron su punto de procedencia con 363 casos, Alemania con 177 casos, China (101), Corea del Sur (99), Canadá (68) y Brasil (67).

Estos datos estadísticos revelan la necesidad de colaboración con organismos y entidades de rango internacional para poder proceder a la detección y eliminación de los casos detectados.

En el caso de S21sec, la colaboración con Symantec es un ejemplo de la lucha conjunta en esta línea. Y es que, gracias a la experiencia acumulada en España, así como en otros muchos países y clientes con los que Symantec cuenta a nivel mundial, S21sec se posiciona como el socio más capacitado para responder a este tipo de amenazas, riesgos y vulnerabilidades de alto nivel.

Gráfico 10: País de procedencia de los casos de phishing en España 2010.



"Estados Unidos sigue siendo la principal fuente de ataques con un 46% del total."

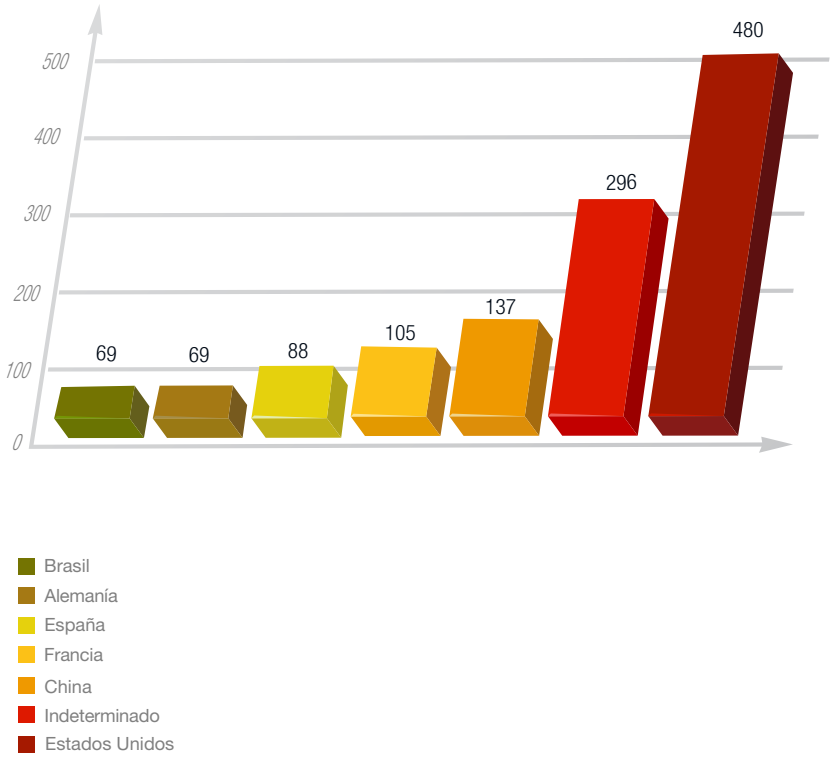
Tampoco hay que dejar de señalar que algunos factores sociopolíticos, económicos y legales influyen poderosamente en la lucha contra el fraude online. Una legislación relajada sobre las responsabilidades de los provedores de servicios de Internet puede dificultar el proceso de cierre de un caso de phishing. De igual modo, la elevada concentración de ISPs en un mismo país puede tener un mismo efecto perjudicial, al provocar unos beneficios marginales menores para las empresas (ISPs y registradores), al hacer que éstas inviertan menos recursos en seguridad.

Códigos maliciosos

En el caso de los códigos maliciosos, los ataques con origen en Estados Unidos siguen siendo los más numerosos con un total de 480 casos, algo más de un 28% de la totalidad, seguidos de aquellos que no revelaron su punto de procedencia con 296 casos, China (137) y Francia (105). Cabe destacar la aparición de España en quinto lugar, y la falta de Rusia, un habitual en pasados años de esta categoría.

Con respecto al tiempo medio de cierre por país, los casos procedentes de Irlanda, Venezuela y Panamá fueron resueltos de forma más rápida con un tiempo inferior a 6 horas. Los casos más difíciles de neutralizar fueron los procedentes de Eslovenia, Chipre y Costa Rica, con un promedio de 192, 188 y 177 horas respectivamente.

Gráfico 11: País de procedencia de los casos de código malicioso en España 2010.

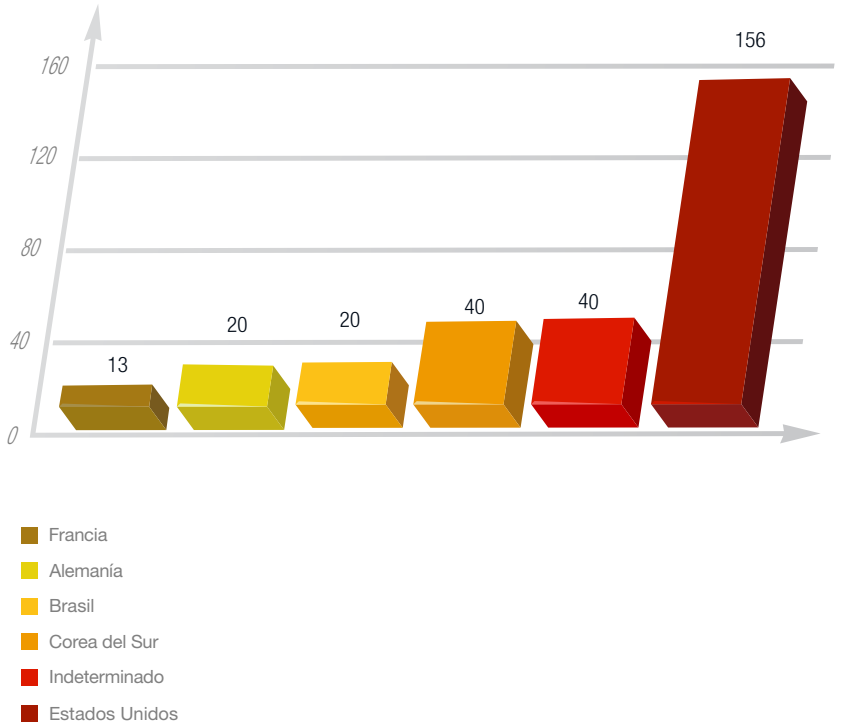


Redirectores

En el caso de los redirectores la mayor parte de los ataques proceden, al igual que en 2009, de Estados Unidos (35%); seguido de aquellos no determinados y Corea del Sur, que sustituye a otros países habituales en esta categoría como Rumanía, Canadá o Reino Unido. También son representativos los índices de Brasil (20), Alemania (20) y por último, Francia (13).

La respuesta más rápida de cierre se registró en los casos procedentes de la India, con apenas veinte minutos de resolución, seguidos de Dinamarca, Perú y Sudáfrica con tiempos inferiores a 6 horas. En el extremo opuesto se sitúa el caso de Chile, con un tiempo de clausura de casi cinco días.

Gráfico 12: País de de procedencia de los casos de redirectores en España 2010.



Evolución del número de ataques en 2010

Como podemos observar en la gráfica, agosto se convierte en el mes que más casos registra con un total de 782 frente a enero que tan sólo registró 277.

Además, durante el mes de agosto, se observa un notable incremento en los ataques de phishing con 442 casos detectados. Comparando estos datos con los recogidos por este mismo informe sobre los ataques de phishing en junio de 2009, observamos cómo en 2010 el nivel se mantiene alto en el mismo periodo. En el lado opuesto destacan los primeros y últimos meses del año, en el que tan sólo se detectaron 145 casos en enero y 250 en diciembre.

En relación a los ataques de código malicioso, en el primer semestre de 2010 se observa una evolución bastante homogénea durante los primeros meses, con un pequeño repunte en el mes de marzo, registrando 173 casos. Luego, la pauta de la tendencia se suaviza, hasta que crece vertiginosamente en agosto convirtiendo este mes en el mes que más ataques se han recibido (295). El año finaliza con un descenso pronunciado y con un bajo nivel en diciembre, con tan sólo 67 casos.

En el caso de los redirectores, se observa un ligero ascenso progresivo en cuanto al número de casos anuales.
Como ocurría en los casos anteriores, el mayor pico de casos se registró en verano, en este caso durante el mes de junio con 48 incidencias.

> *"El número de casos de phishing, código malicioso y redirectores se ha incrementado progresivamente durante el primer semestre de 2010, descendiendo casi a sus niveles iniciales en los meses finales del año."*

Gráfico 13: Evolución de los casos totales por mes.

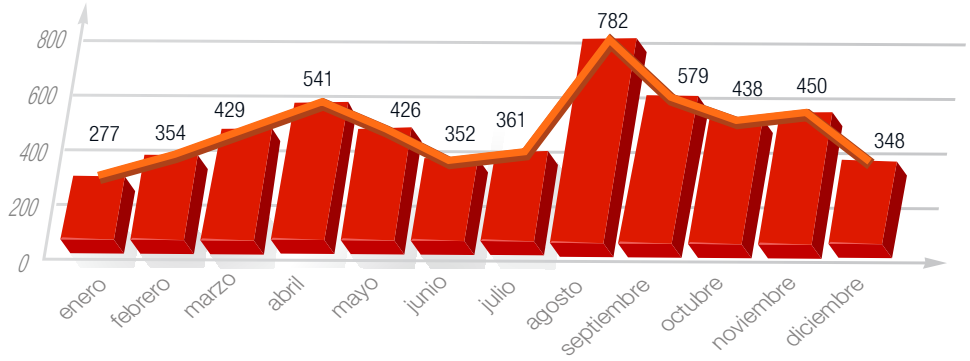


Gráfico 14: Evolución de los casos de phishing por meses 2010.

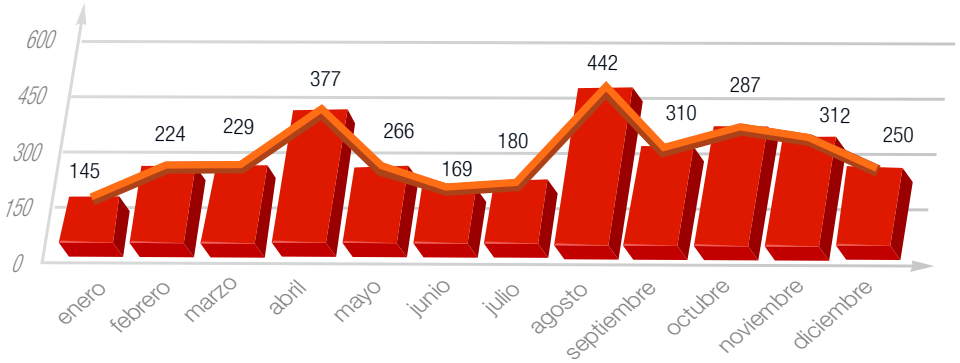


Gráfico 15: Evolución de los casos de código malicioso por meses 2010.

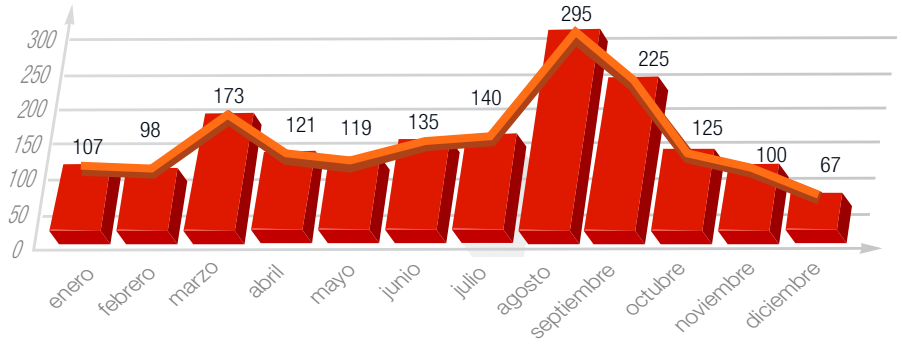
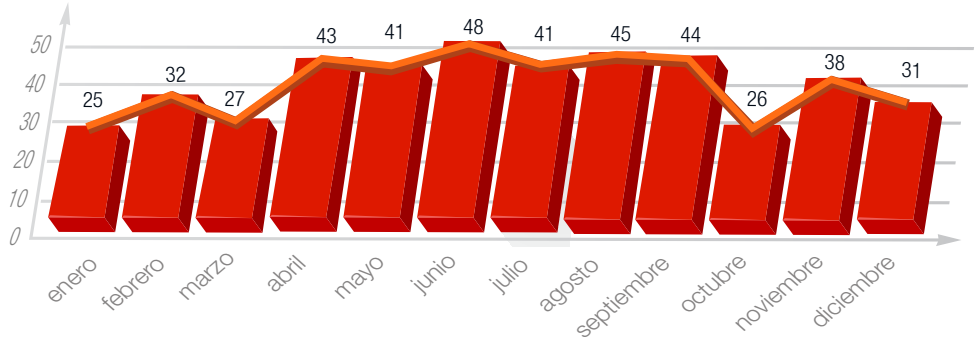


Gráfico 16: Evolución de los casos de redirectores por meses 2010.



Evolución

Evolución de los distintos tipos de fraude desde enero 2005 hasta diciembre 2010

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

Gráfico 17: Total casos de fraude desde marzo 2005 hasta diciembre 2010.

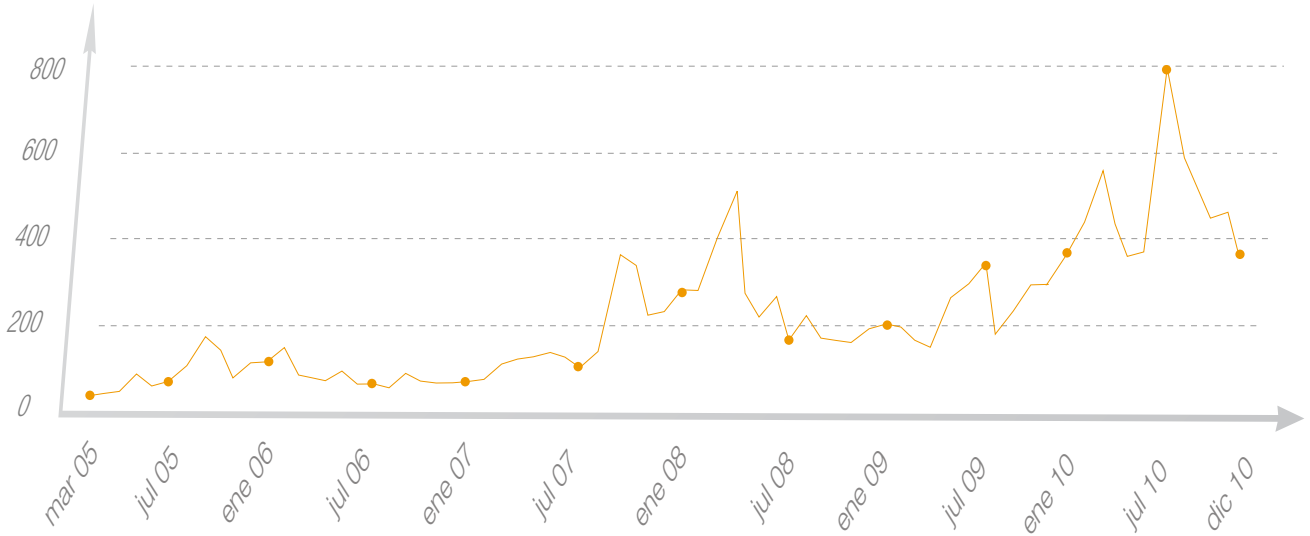


Gráfico 18: Total casos de phishing desde marzo 2005 hasta diciembre 2010.

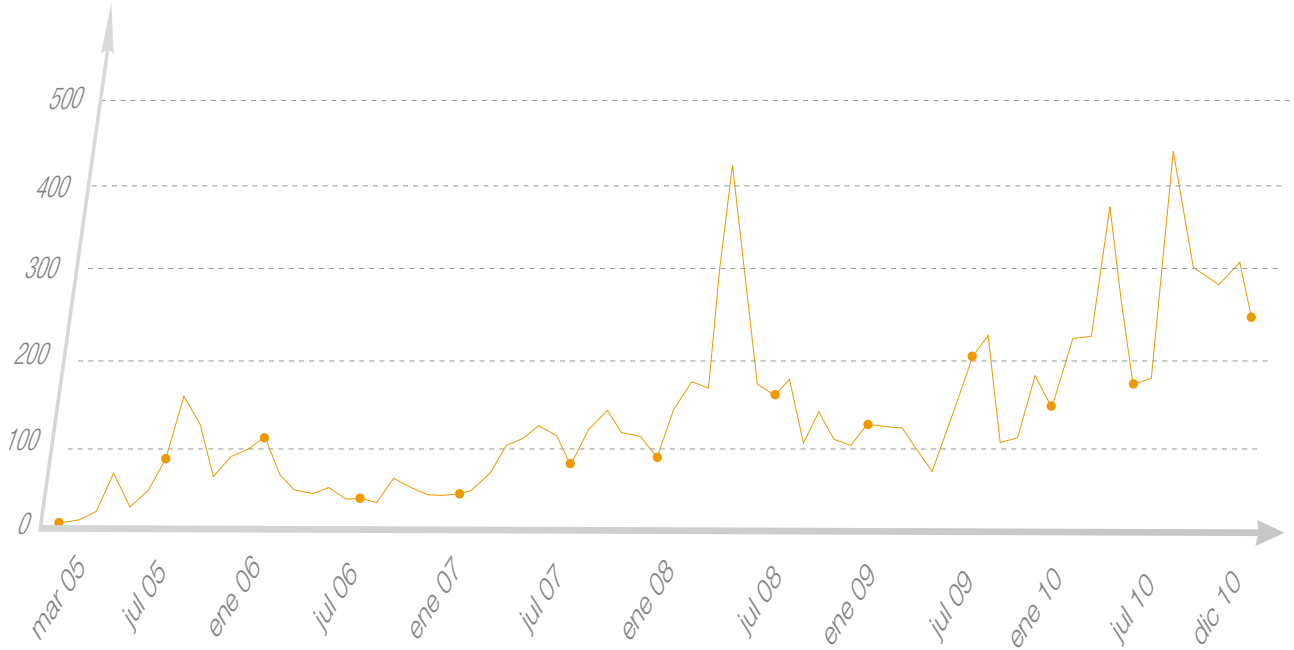


Gráfico 19: Total casos de código malicioso desde enero 2006 hasta diciembre 2010.

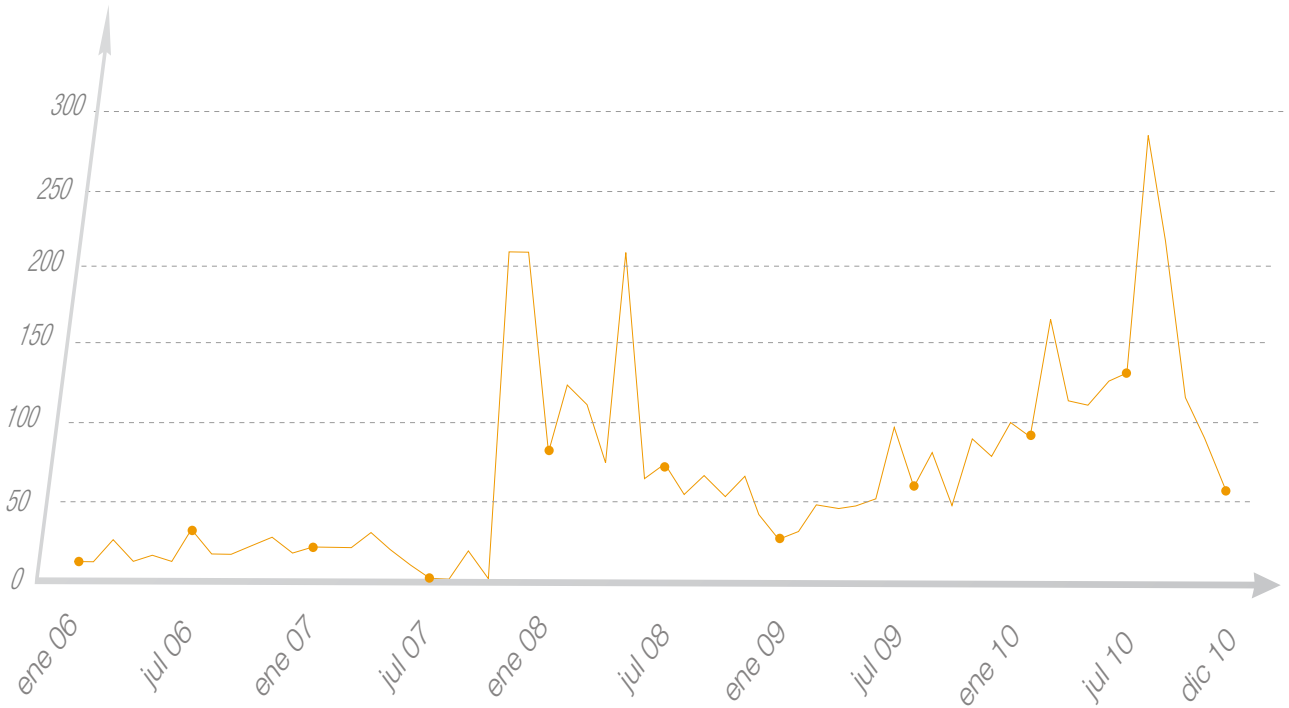
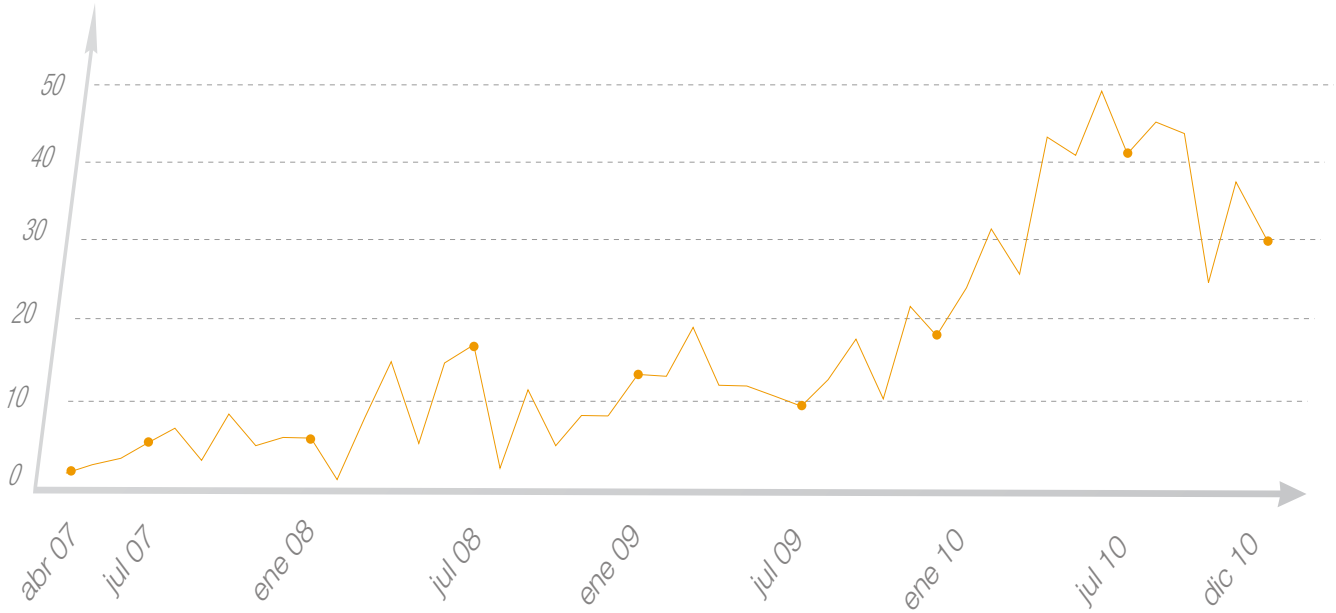


Gráfico 20: Total casos redirectores de abril 2007 a diciembre 2010.



Cronología 2010

Cronologia 2010

Enero

La “Operación Aurora” implicó el “descubrimiento” de un 0-day en Internet Explorer que afectaba potencialmente a millones de usuarios, además de suponer una acusación directa de espionaje industrial de Estados Unidos a China.

En lo relativo a tecnología móvil, durante este mes aparecieron las primeras muestras de malware bancario afectando a los cada vez más populares móviles con Android, y el cifrado 3G era comprometido.

En cuanto a vulnerabilidades web, se destacó la sonada vulnerabilidad de Cross-site scripting en la web de la Presidencia Europea y el defacement realizado en la web del ministerio de vivienda.

Febrero

La empresa norteamericana NetWitness publicó un informe de un gran impacto mediático. Dicho informe mostraba la aparición de un troyano que había infectado a más de 74.000 ordenadores en todo el mundo y robado información de acceso a los sitios de más de 2500 entidades de gran cantidad de países. Finalmente se trataba de una nueva versión de Zeus.

Por otra parte, se anunciaba el cierre de la Botnet Wadelac por parte de Microsoft. Wadelac era una de las principales responsables de envío de SPAM a nivel mundial formando parte de algunas campañas de distribución de troyanos como Zeus mediante correos de San Valentín.

Una de las noticias más destacadas de febrero fue la publicación de una vulnerabilidad en el protocolo de las tarjetas EMV, concretamente en la fase de autenticación de usuario y a través de un ataque MitM para devolver siempre un PIN válido.

S21sec fue protagonista en diferentes medios a raíz de la charla “Playing in a satellite environment” en la Black Hat DC, en la cual se puso de manifiesto la escasa seguridad en algunas comunicaciones vía satélite.

Marzo

La desarticulación de la Botnet Mariposa por parte del grupo de Delitos Informáticos de Guardia civil fue la noticia más notable en cuanto a lucha contra el fraude a nivel mundial. Dicha Botnet era administrada desde España y disponía de más de 13 millones de equipos infectados.

Este mes también se mostraron dos nuevos vectores de distribución de código malicioso: a través de las baterías USB recargables de Energizer, cuyo software incluía la instalación de un troyano, y la distribución del troyano Mariposa entre otros, a través de los móviles HTC de Vodafone.

El troyano SpyEye empieza a aparecer en escena con un gran potencial de crecimiento y el troyano ZeuS empieza a implementar funcionalidades de MitB

Abril

Godaddy uno de las mayores empresas de hosting fue víctima de un ataque masivo afectando a una cantidad importante de blogs comprometidos en sus sistemas.

En la conferencia HITB se hizo una presentación sobre ataques a cajeros automáticos y en este mismo sentido Bank of América acusó a uno de sus empleados de instalar código malicioso en sus cajeros automáticos.

El proyecto Apache sufrió una intrusión en sus sistemas a raíz de un Cross-site scripting en el sistema de ticketing de Jira.

Una actualización de McAfee provocó que los equipos detectasen el proceso svchost.exe como malicioso provocando que los equipos se reiniciaran continuamente o la aparición de un BSOD.

El troyano ZeuS sigue imparable incorporando nuevas funcionalidades. Y aparece en escena un nuevo troyano conocido como Mebratix.B, que se instala en la MBR del equipo infectado.

Mayo

Una nueva técnica susceptible de ser usada en ataques phishing aparece en escena por parte de Aza Raskin, experto en desarrollo de interfaces gráficas. La técnica denominada Tabnapping se aprovechaba de la costumbre de todos los usuarios de mantener abiertas gran cantidad de pestañas en el navegador.

El hackeo del foro carders.cc y el ciberdelincuente ruso que robó credenciales de 1.5 millones de cuentas en Facebook fueron las noticias más destacadas este mes.

Junio

Una de las noticias más polémicas fue la publicación de la vulnerabilidad en el protocolo HCP de Microsoft y reportada por Tavis Ormandy, la polémica vino por el escaso margen que se dio para su solución antes de hacerla pública.

A nivel empresarial en España se detuvo a tres gerentes de una empresa que comercializaba con software que incorporaba "bombas lógicas", poniendo así en tela de juicio la confianza de las empresas en relación a sus proveedores de software.

Las redes sociales como Twitter y Youtube, fueron una de las vías de propagación favoritas para realizar una campaña masiva de SPAM cuyo objetivo era la distribución de un troyano Zeus con una tasa de detección muy baja.

El mundial de futbol fue usado en una campaña de propagación de malware a través de técnicas Black Hat SEO y el troyano ZeuS se consolidaba en su versión 2.

Julio

El gusano STUXNET hizo su aparición, su principal objetivo el ataque a sistemas SCADA de Irán e Indonesia a través de la vulnerabilidad LNK que afectaba a sistemas Microsoft.

Las campañas de distribución de ZeuS no cesan y entra en escena un binario de la rama 1.3. Se detectaron también algunas muestras de Sinowal afectando a entidades españolas.

Una de las detenciones más sonadas del mes fue la del creador de la Botnet Mariposa, cuyos administradores ya habían sido detenidos en marzo.

Agosto

La empresa norteamericana NetWitness publicó un informe de un gran impacto mediático. Dicho informe mostraba la aparición de un troyano que había infectado a más de 74.000 ordenadores en todo el mundo y robado información de acceso a los sitios de más de 2500 entidades de gran cantidad de países. Finalmente se trataba de una nueva versión de ZeuS.

En el escenario móvil apareció el primer troyano para Android que realizaba envíos de SMS a números de tarificación especial. En la conferencia de Seguridad Defcon se presentó el procedimiento para liberalizar el iPhone4 y la interceptación de llamadas con el protocolo GSM.

ZeuS siguió siendo el troyano bancario más predominante en los usuarios españoles.

Septiembre

S21sec e-crime descubrió el primer troyano capaz de evitar la autenticación de dos factores, bautizado como ZeuS-MitMo al tratarse de una muestra de un ZeuS 2.x que inyectaba HTML para conseguir el teléfono de la víctima con el objetivo de obtener el SMS con el TAN para su reenvío.

La red social Twitter se vio afectada por una vulnerabilidad Cross-site Scripting que permitía hacer retweets con tan solo pasar el ratón por encima de un enlace (evento onmouseover).

Octubre

El troyano SpyEye incorporó técnicas Man in the Browser contra entidades españolas.

La red social LinkedIn fue víctima de una campaña de SCAM para distribuir ZeuS.

Se descubrió una vulnerabilidad en los teléfonos iPhone que permitía mediante una combinación de teclas, realizar llamadas desde un teléfono bloqueado.

Noviembre

Un joven de Sevilla fue detenido por la Guardia Civil al conseguir infectar a más de 300 usuarios de la red social Tuenti a través de código malicioso.

El troyano Qakbot fue el responsable de varios fraudes realizados en USA sobre cuentas corporativas, disponía de características prácticamente únicas que lo diferenciaban de la gran mayoría del malware bancario.

Una gran operación conjunta desarrollada durante meses entre policías de USA y Moldavia culminó con la detención de todos los escalones de la red de una banda internacional dedicada al fraude informático mediante el clásico esquema de troyanos ZeuS.

Diciembre

Dos de las mayores plataformas de publicidad online: DoubleClick y MSN fueron víctimas de malvertising.

El proyecto OpenBSD se vio envuelto en un escándalo por la existencia de puertas traseras originadas por el FBI a través de empresas que contribuían con código.

Los hechos originados por WikiLeaks y los ataques DDoS a grandes corporaciones se llegaron a calificar como la primera ciberguerra de la historia.

Conclusión y tendencias de futuro

Conclusión y tendencias de futuro

Las estadísticas de 2010 demuestran que no ha sido un año de grandes cambios en cuanto a la tipología de los incidentes de fraude se refiere, aunque sí se ha observado un aumento considerable en el número de incidentes. Hoy en día, el phishing sigue siendo una amenaza utilizada a menudo, aunque quizás ya no enteramente dirigida a las entidades financieras, sino también a otros sectores con el objetivo de robar información confidencial (principalmente relacionado con los datos de una tarjeta de crédito). Sectores como el del transporte, el del comercio online o, incluso, cualquier asociación pueden ser utilizados para la obtención de dichos datos personales.

Al fin y al cabo, la ingeniería social sigue siendo la técnica que mejor funciona a la hora de robar datos personales. No hace falta tener ningún conocimiento técnico ya que basta con, simplemente, escoger un tema que resulte atractivo (un sorteo, lotería, un viaje gratis, etc.), para que muchas personas piensen que es 100% real. El phishing tiene una parte importante de ingeniería social y otra parte, no menos importante, que consiste en gestionar los datos robados para conseguir rentabilidad (cash out) y dinero real, a partir de los mismos. En nuestro caso, durante 2010 no ha habido grandes cambios en ambas facetas, y tanto las excusas de seguridad como la utilización de mulas siguen siendo métodos principales para llevar a cabo acciones de fraude.

En general, durante 2010 no se aprecia un patrón relacionado directamente con el aumento o descenso del número de incidentes de fraude a lo largo de los meses, excepto un ascenso de los mismos durante los meses estivales. Aunque sí que existe una relación muy fuerte entre el número de incidentes que sufre una organización y las medidas de seguridad que ésta implementa. Por ejemplo, existe un hecho muy característico que hemos podido comprobar en varias organizaciones en todo el mundo, que es la relación causa-efecto entre el uso de algún factor de autenticación fuerte (por ejemplo, un OTP) y el descenso absoluto de los incidentes de phishing. Realmente, es casi inmediata la desaparición de los incidentes de phishing 'clásicos' una vez que existe alguna de estas soluciones (aunque la marca de la organización se siga usando para el robo de otros datos personales).

Otra causa-efecto muy visual que hemos detectado durante 2010 es la que afecta a los proveedores de hosting (ISPs) relacionados con el fraude. En el mismo momento en que se consigue que esos ISPs estén fuera de Internet, el número de incidentes casi desaparece por completo (tanto en phishing como con códigos maliciosos). Es decir, que tanto las medidas que se imponen desde las entidades afectadas como las medidas aplicadas en terceros influyen notablemente en el número de incidentes. Por ello, desde S21sec trabajamos con la confianza de nuestros clientes para ayudarles a implementar todas las medidas de seguridad necesarias para eliminar este riesgo y hacer frente a todas las organizaciones criminales que se esconden detrás de estos incidentes.

En el caso del código malicioso, tampoco se han experimentado grandes cambios, aunque sí que hay algunos más que en 2009. La familia de ZeuS ha seguido siendo el código malicioso relacionado con el fraude que más incidencias ha tenido, principalmente en Europa, Estados Unidos y Australia, mientras que en Latinoamérica sigue existiendo el código malicioso 'local' que paulatinamente va ganando en complejidad, pero sin llegar a la complicación del código procedente de Europa del Este.

SpyEye por fin ha terminado de madurar, y durante 2010 ya se han registrado un gran número de incidentes provocados por él. Además, otras familias de reciente creación como Carberp poco a poco empiezan a desplegar sus redes. También en 2010 las plataformas móviles se han convertido en un objetivo para los atacantes, puesto que se ha podido observar código malicioso con objetivos puramente fraudulentos para iPhone (iKee), BlackBerry (ZeuS), Windows Mobile (ZeuS), Symbian (ZeuS) e incluso para Android (con multitud de ejemplos, quizás la plataforma más atacada).

Como todos los años, el país que alberga la mayoría de los incidentes de fraude (phishing y código malicioso) sigue siendo Estados Unidos, aunque en muchas ocasiones son máquinas comprometidas y no ISPs dedicados al fraude (bullet-proof hosting), puesto que la mayoría de estos bullet-proof ISPs se encuentran en otros países. De hecho, es en el momento en el que se consigue desconectar a estos ISPs de Internet cuando se alcanzan esos descensos tan pronunciados del número de incidentes. Un caso particular fue el que vivimos en septiembre relacionado con el ZeuS Man-in-the-Mobile (ZeuS Mitmo, recomendamos su lectura en nuestro blog), donde se alojaba el código malicioso en un ISP holandés (hasta aquí todo normal), pero enviaba los SMS que interceptaba a lo que parecía un número británico (con el prefijo +44).

Después de poder hablar con los operadores móviles de Inglaterra, se descubrió que era un número que se había subcontratado varias veces de forma encadenada. Finalmente, el origen se encontraba en la Isla de Guernsey, una pequeña isla en medio del Canal de la Mancha que no pertenece a la Unión Europea, con lo que el acceso a los datos se complica de forma casi exponencial.

Durante 2010 y principio de 2011 hemos podido comprobar cómo se tambaleaban muchas de nuestras percepciones de seguridad, al ver cómo grandes empresas de seguridad eran comprometidas. También muchas de las aplicaciones o servicios que considerábamos seguros han sufrido incidentes muy graves que hacen peligrar su seguridad. Éste es el caso de HBGary, RSA, PHPFog o Comodo, y es seguro que durante 2011 seguiremos viendo más incidentes. Incidentes que algunas veces se relacionan con aspectos puramente políticos, pero que muchas veces no son más que ataques puramente técnicos, sin ninguna teoría de la conspiración.

En definitiva, el año 2010 ha sido un año parecido a los anteriores, donde ya se ha destapado la caja de Pandora de los dispositivos móviles (incluyendo a los tablets), y que será también recordado como el año que ha supuesto un punto de inflexión en la seguridad. La desconfianza ha aumentado significativamente, sobre todo como consecuencia de los ataques a empresas, pero también por esa falsa sensación de seguridad que podemos tener. Si a este hecho le sumamos la crisis económica y la desconfianza entre países, todo apunta a que 2011 será un año en el que el número de incidentes de seguridad crecerá, pero también la complejidad y los daños ocasionados por los mismos.

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 *ecrime@s21sec.com* o a través de nuestra web *www.s21sec.com*.

Spain • Mexico • Brazil • UK • USA

S21sec e-crime