Informe anual PandaLabs

Resumen 2011

01| Introducción

En este informe Trimestral incluimos un repaso a lo más destacado de lo sucedido en el panorama de seguridad del año 2011. Podréis encontrar las cifras del año de creación de malware e infecciones, donde podemos ver que este año se ha batido un nuevo récord con la creación de 26 millones de muestras de malware.

Hablaremos de las redes sociales, donde Facebook sigue reinando tanto en número de usuarios como en número de ataques. También daremos un repaso a lo sucedido en el mundo de la telefonía móvil y las tablets, donde Android se posiciona como el sistema operativo preferido de los ciberdelincuentes.

Pero si algo debemos destacar de este año 2011, es que se ha convertido en el año de los ciberataques. Hemos sido testigo del mayor robo de datos de la historia, con la compañía Sony como gran protagonista, ya que fue en su PlayStation Network donde se perpetró un robo de datos de millones de sus usuarios. Este no fue el único percance que tuvieron, y en total le han robado a Sony datos de más de 100 millones de usuarios. Otra plataforma de juegos, Steam, fue víctima de un ataque en el que se comprometió la información de más de 35 millones de personas.

La ciberguerra ha sido protagonista también este año. En 2011 han tenido lugar ataques en todo el mundo, afectando a gobiernos de todos los lugares y colores. Este tipo de ataques no sólo son sufridos por los gobiernos, sino que también afectan a compañías relacionadas con los mismos, como fabricantes armamentísticos.

En este informe encontraréis los casos más destacados ocurridos a lo largo de 2011, así como una mirada al futuro donde trataremos de vaticinar qué nos espera en este año lleno de incertidumbres.

02| 2011 de un vistazo

Las redes sociales ocupan un lugar importantísimo en la vida de los internautas, siendo los reyes en esta materia Facebook y Twitter. Este año ha entrado con fuerza un nuevo jugador que trata de competir con Facebook, Google+.

Redes Sociales

GOOGLE+.

A pesar de su rápido crecimiento, consiguiendo millones de usuarios en unos pocos meses, aún está muy lejos de su directo competidor, Facebook, lo que hace que la mayor parte de los ciberdelincuentes no hayan mostrado interés en utilizar Google+ para distribuir sus creaciones. Sin embargo cabe mencionar un caso curioso: al poco tiempo de lanzarse esta nueva red social, como las invitaciones no estaban abiertas a todo el público y había mucha expectación y ganas por parte del público de conseguir la suya, vimos un caso muy curioso que tuvo lugar… en Facebook. Crearon una página llamada "Get Google Plus Invitation FREE" (Consigue gratis invitación a Google Plus) donde sólo tenías que dar a "Me gusta" para conseguir dicha invitación. Por supuesto, también había que facilitar la dirección de correo para que te pudieran enviar dicha invitación, aunque realmente se trataba de un engaño y dicha invitación no existía.

TWITTER

Respecto a la red social que reinventó los mensajes cortos, Twitter, debemos decir que no ha sufrido un aumento de ataques respecto al año 2010. Aunque sigue habiendo ataques que utilizan los "Trending Topics" como gancho para distribuir links maliciosos, hemos visto menos casos, quizás por el mejor trabajo de filtrado que viene realizando el equipo de Twitter. En cualquier caso seguimos viendo cómo se sigue utilizando como plataforma de envío de mensajes de spam, pero si hay un aspecto

en el que podamos destacar a la red social respecto a ataques es el hackeo de cuentas. Así, vimos como la cuenta de Twitter de Fox News fue hackeada y comenzó a publicar el 4 de julio, una falsa noticia anunciando la muerte de Obama. También hemos visto como la cuenta de PayPal UK fue hackeada comenzando a enviar mensajes en tono jocoso riéndose de la seguridad que tienen.

Pero no todos estos ataques son realizados en plan bromista, ya que vimos hackeo a la cuenta de Twitter de una entidad financiera, donde los ciberdelincuentes comenzaron a enviar DMs (mensajes directos) a los seguidores de su cuenta, indicándoles que debían pinchar en un link debido a un problema de seguridad en su cuenta. Este link dirigía al usuario a una página de phishing que imitaba la del banco, donde le solicitaba todos los datos necesarios para poder posteriormente hacerse pasar por dicho cliente y robarle el dinero.

FACEBOOK

Cuando hablamos de ataques en Facebook, tendemos a pensar que simplemente los ciberdelincuentes utilizan la plataforma para distribuir malware, pero la verdad es que no es así, Como muchas veces hemos comentado, la gente publica demasiada información personal en sus perfiles, lo que facilita el "hackeo" de cuentas de correo electrónico y del mismo Facebook. George S. Bronk ha sido detenido en California precisamente por llevar a cabo este tipo de actividades. Utilizaba la información disponible en Facebook para hacerse con la cuenta de correo electrónico de la víctima. Una vez "secuestrada" la cuenta, buscaba información personal con la que hacer chantaje y obtener así dinero.

Y parece que cualquiera puede ser víctima de estos ataques, ya que el propio Mark Zuckerberg – creador de Facebook- ha sido víctima de un ataque de este tipo, y su página de fans de Facebook fue hackeada, mostrando un mensaje que comenzaba con "Let the hacking begin".

FIG.01. *IMAGEN DE LA PÁGINA REAL DE MARK ZUCKERBERG, CREADOR DE FACEBOOK, TRAS SER HACKEADA.*

El mundo de las redes sociales deja claro que los usuarios somos capaces de chocar con la misma piedra una y otra vez. Hemos visto como las típicas campañas en Facebook de "Descubre quién visita tu perfil" y similares consiguen un gran éxito afectando a miles de usuarios cada vez.

Este tipo de engaños, de hecho, está muy extendido en Facebook, la plataforma favorita de los delincuentes para lanzar sus ataques mediante técnicas de ingeniería social, siempre usando noticias reales o bulos en los que muchísimos usuarios siguen cayendo.

Además, técnicas que se utilizaban en otros ámbitos, como el uso de noticias recientes para engañar a los usuarios también tienen su lugar aquí. Sin ir más lejos, en cuanto se supo que Steve Jobs había fallecido, fue creada una página de Facebook llamada "R.I.P. Steve Jobs", y miles de usuarios inocentes se unieron a la misma. En pocas horas llegaron hasta los 90.000 seguidores. Los cibercriminales publicaron un link usando el popular acortador de URLs bit.ly, diciendo que Apple regalaría 50 iPads.

Como es de imaginar, esto no era más que una estafa, y una vez que el usuario hacía click en la url (la cual terminaba en "restinpeace-steve-jobs") se le redirigía a un sitio web en el que se ofrecían diferentes regalos, como iPads o televisores Sony Bravia. Para acceder a ellos se le pide información al usuario, como el nombre, número de teléfono móvil, dirección de e-mail, etc.

FIG.02. *PÁGINA CREADA EN FACEBOOK PARA APROVECHARSE DEL FALLECIMIENTO DE STEVE JOBS.*

Ciberdelincuencia

El objetivo de los ciberdelincuentes es robar información que luego puedan convertir en dinero. Es por ello que los troyanos bancarios, aquellos diseñados para robar información a los clientes de entidades financieras, sean una de sus armas preferidas, pero en ocasiones vemos otro tipo de ataques. En enero, The Pentagon Federal Credit Union denunció que a través de un PC infectado se accedió a una de sus bases de datos con información confidencial de sus clientes. Entre la información robada se encontraban nombres, direcciones, números de seguridad social e información sobre cuentas y tarjetas de crédito.

Otra práctica habitual que no está relacionada con malware, es el uso de dispositivos de copia de tarjetas de crédito utilizados en cajeros. En enero se condenó a dos hombres de 32 y 31 años de edad por este hecho, a 7 y 5 años de cárcel respectivamente. Se sospecha que pertenecen a una banda de criminales rusos y americanos que están operando en todo el país.

Pero no sólo es el sector bancario el que se enfrenta al peligro. Tras un robo en la República Checa y un intento de pirateo en Austria, la Comisión Europea se vio obligada a suspender el sistema de comercio de derechos de emisión de CO2. Por supuesto, los ciberdelincuentes buscaban un beneficio económico. Ya se dio un ataque similar hace unos meses, cuando un pirata informático robó 1,6 millones de derechos de emisión a la cementera Holcim en Rumanía. A 15 euros cada uno, suponía unas pérdidas de 24 millones de euros. En este tipo de ataques, además de las pérdidas económicas, es el propio sistema el que se ve atacado y muestra su vulnerabilidad.

Esta diversificación se puede ver en otros ámbitos. Este año hemos visto cómo aparecían variantes del conocido troyano bancario ZeuS cuyo objetivo no eran entidades bancarias, sino sistemas de pago online como Webmoney o MoneyBookers.

Otro ataque que ha tenido lugar tuvo como víctima de ZeuS al gobierno británico, que reconoció haber sido infectado tras recibir un ataque dirigido que contenía una versión de este troyano que, además de estar preparado para robar credenciales bancarias, puede robar todo tipo de información de la víctima.

En marzo, RSA hizo público que habían detectado una intrusión que había conllevado el robo de información sobre el diseño de su conocido sistema de doble factor de autenticación "SecureID".

FIG.03. *RSA SUFRIÓ UNA INTRUSIÓN EN MARZO.*

En mayo Lockheed Martin, el primer contratista del Departamento de Defensa de Estados Unidos sufrió una intrusión gracias al uso de la información robada meses atrás a RSA. Parece que los que robaron la información han conseguido comprometer el algoritmo utilizado para generar las claves, teniendo RSA que cambiar los más de 40 millones de SecurID que tienen sus clientes, entre los que se encuentran las más importantes empresas del mundo. Meses más tarde RSA dijo que estaba convencida que había algún gobierno detrás del ataque que sufrieron, y el popular blogger de seguridad Brian Krebs desveló en octubre un listado de 760 empresas que podrían haber sido afectadas por el mismo atacante.

En junio se descubrió que el Fondo Monetario Internacional había estado comprometido durante meses, aunque debido a la escasa información que se ha hecho pública desconocemos la motivación detrás del ataque. Es bastante probable, debido al tipo de delicada información que maneja la institución, que se trate de un ataque dirigido. Sin embargo tampoco podemos descartar que se trate de un caso de cibercrimen común.

El sitio web de la Agencia Espacial Europea fue hackeada y todos los datos robados fueron hechos públicos. Entre los datos se encontraban nombres de usuario, cuentas ftp, e incluso las contraseñas de las cuentas ftp que se encontraban ¡en texto plano!

Citigroup ha protagonizado otro incidente vergonzoso, donde información de 360.000 cuentas ha sido comprometida. Lo peor de este ataque, es que ni siquiera hubo la necesidad de hackear un servidor, simplemente "jugando" con la URL podías acceder a la información de otra cuenta.

Sega, la popular compañía japonesa de videojuegos, ha sido otra de las víctimas: los datos de 1,3 millones de usuarios de su red Sega Pass fueron robados el pasado mes de junio, incluyendo nombres de usuario, fechas de nacimiento, direcciones de correo y contraseñas, aunque éstas estaban cifradas, por lo que se minimiza algo el riesgo si el cifrado utilizado es fuerte, algo que vistas experiencias pasadas no está suficientemente extendido.

Pero si hay un ataque que debe figurar en el muro de la vergüenza, es el que sufrió Sony. Empezó con el robo de datos en su red PlayStation Network (PSN) que afectó a los datos de 77 millones de usuarios de todo el mundo. No sólo se trata del mayor robo de datos de usuarios de la historia, sino que el manejo que hizo la compañía fue catastrófico: ocultó el problema durante días, y cuando lo hizo público dijo que datos de usuarios podrían haber sido comprometidos cuando sabían fehacientemente que habían sido robados.

FIG.04. *DATOS DE MILLONES DE USUARIOS DE PSN FUERON ROBADOS EN 2011.*

Para agravar aún más la situación, los datos robados eran especialmente sensibles, ya que incluían el nombre, dirección completa del usuario, dirección de correo electrónico, ID de PSN, contraseña (todo parece indicar que no estaba cifrada), fecha de cumpleaños, historial de compras, nº de la tarjeta de crédito (sólo de los usuarios que tenían almacenada esta información, se calcula que es un 10%), fecha de caducidad de la misma… Si esto no fuera suficiente, días después sufrió otro ataque Sony Online Entertainment, sufriendo un robo de datos similar que afectó a otros 24 millones de usuarios.

En julio, Rogelio Hackett, de 25 años, fue condenado a 10 años de cárcel y pagar una multa de 100.000$ por haber robado datos de 675.000 tarjetas de crédito. El hablar de condenas en firme es un paso muy importante, ya que es una de las mejores medidas disuasorias que muestran que la impunidad no es una opción.

Para tratar de infectar y robar información a los usuarios, los ciberdelincuentes utilizan técnicas de ingeniería social, y como siempre en cuanto se produce alguna noticia relevante tratan de aprovecharse de la misma, como ha sido el caso del fallecimiento de la cantante Amy Whinehouse o el de Steve Jobs.

En noviembre, ciberdelincuentes consiguieron acceder a la base de datos de clientes de Steam, la popular plataforma de juegos de Valve, con lo que la información de más de 35 millones de personas fue robada, incluyendo números de tarjetas de crédito y contraseñas. Afortunadamente, estos dos datos se encontraban cifrados, por lo que el riesgo de que los ladrones puedan acceder a la información real disminuye notablemente.

FIG.05. *DATOS DE 35 MILLONES DE USUARIOS DE STEAM FUERON ROBADOS EN NOVIEMBRE.*

Una de las claves en la lucha contra la ciberdelincuencia es la colaboración entre los diferentes países, ya que la mayoría de los delitos se dan en diferentes países al no existir fronteras en Internet. A este respecto, una buena noticia la tuvimos este año cuando el US-CERT y el CERT-In (de Estados Unidos e India respectivamente) firmaron un acuerdo de colaboración que abre un rayo de esperanza. Si acuerdo de este tipo se generalizan podría suponer un importante paso adelante en la lucha contra la delincuencia en Internet.

A pesar de que la mayoría de robos buscan el dinero, no siempre es así. De hecho, este año hemos sido testigos sobre varias famosas que han sido víctimas de robo de fotos personales en las que posaban desnudas (siendo sin duda el caso más llamativo el de Scarlett Johansson, de la que aparecieron fotos posando desnuda que ella misma se había tomado con su teléfono móvil). Se llegó a especular que un grupo organizado podría estar detrás de estos ataques, realizando hackeos de los teléfonos móviles a través de vulnerabilidades desconocidas, pero la realidad resultó ser mucho más sencilla. Se detuvo al responsable de estos ataques, Christopher Chaney, de 35 años, y confesó todo: se había "colado" en el correo electrónico de sus víctimas adivinando su contraseña. Y no es que fuera vidente, sino que sus víctimas usaban información personal suya como parte de su contraseña, con lo que con un poco de paciencia pudo averiguar la correcta y acceder al correo personal. Además no podemos decir que tuviera mal gusto ya que además de Scarlett Johannson, entre las 50 celebridades se encontraban personajes de la talla de Jessica Alba, Vanessa Hudgens, Miley Cyrus o Christina Aguilera. Lamentablemente, la mayoría de los usuarios crean sus contraseñas de la misma forma, lo que aumenta el riesgo de que alguien pueda dar con la adecuada y acceder a nuestra información más personal.

FIG.06. *CHRISTOPHER CHANEY, DE 35 AÑOS DE EDAD, RESPONSABLE DEL ROBO DE FOTOS PERSONALES DE 50 CELEBRIDADES.*

Ciberguerra

Este ha sido uno de los temas estrella, se han producido tantos casos que podríamos escribir una enciclopedia sólo con lo ocurrido durante 2011 en el campo de la ciberguerra o ciberespionaje. Vivimos en una era en la que todo y todos estamos conectados a Internet, lo que representa grandes oportunidades a los amantes de la información ajena, por lo que todo tipo de agencias y gobiernos están trabajando activamente en este campo.

En **enero** se supo que un ataque dirigido había alcanzado de lleno al Ministerio de Economía canadiense. Las primeras investigaciones apuntaban a China, si bien es cierto que es muy difícil demostrar quién estaba realmente detrás del ataque. No se ha hecho pública qué información ha sido robada.

En **febrero** la compañía americana McAfee hizo público un informe en el que se hablaba de la operación "Night Dragon", donde una serie de compañías energéticas habían sido víctimas de espionaje en una operación que había estado activa al menos durante dos años. Posteriormente se ha podido conocer que entre las compañías víctimas del ataque se encontraban Exxon Mobil, Royal Dutch Shell, BP, Marathon Oil, ConocoPhillips, y Baker Hughes. Los ataques, de nuevo, venían desde China, aunque no se puede demostrar que el gobierno Chino esté directamente implicado.

En **marzo**, se conoció que ordenadores militares de Noruega habían sido atacados en marzo: unos 100 militares –muchos de ellos de alto rango- recibieron un correo electrónico en noruego, que incluía un fichero adjunto. Este fichero era un troyano creado para robar información. Según la información hecha pública, uno de los ataques tuvo éxito aunque desde ese ordenador no se tenía acceso a información crítica.

En el mismo mes se hizo público que el Ministerio de Economía francés fue víctima de otro ataque varios meses antes –cuyo origen apunta de nuevo a China- cuyo objetivo era el robo de documentos sobre la reunión del G-20 en febrero, que tenía lugar en París. Más de 150 ordenadores estaban afectados, y otros ministerios franceses habían sufrido intentos de intrusiones sin éxito.

También en marzo, 40 páginas web pertenecientes principalmente al gobierno de Corea del Sur, fueron víctimas de un ataque de denegación de servicio. Este ataque ha sido muy similar a otro que tuvo lugar en 2009, del que se culpó a Corea del Norte, pero tras la investigación todo apuntaba a… China.

En **mayo** el portavoz del ministerio de defensa de China, Geng Yansheng, confirmó que tenían una unidad de élite de ciberguerreros. Diferentes fuentes de inteligencia del Reino Unido comentaban que dicho equipo había sido formado al menos hacía 2 años. A finales del mismo mes, el Pentágono declaraba que cualquier tipo de ciberataque llevado a cabo por un gobierno extranjero puede ser clasificado como un acto de guerra.

En **julio**, el adjunto al secretario de defensa estadounidense, Bill Lynn, hizo público un ataque recibido en marzo, durante el que habían robado 24.000 documentos pertenecientes a un sistema armamentístico secreto. El DoD dijo que lo más posible es que se tratara de un ataque perpetrado por el servicio de inteligencia de una potencia extranjera.

FIG.07. *EL DEPARTAMENTO DE DEFENSA DE ESTADOS UNIDOS SUFRIÓ UN ROBO DE 24.000 DOCUMENTOS.*

Unos días más tarde, el general de los Marines James 'Hoss' Cartwright hizo unas declaraciones en las que decía que el departamento de IT del DOD estaba en la edad de piedra.

Si algo se puede decir de los ataques de ciberguerra o ciberespionaje, es que en la mayoría de los casos se mira hacia China como la gran sospechosa que está detrás de todos ellos. Sin embargo es obvio que por una parte China no es la responsable de todos los ataques, y por otra en China tienen que estar recibiendo ataques. Una de las características que distinguen a un país democrático de uno que no lo es, es la información que se hace pública a sus ciudadanos. Cuando por ejemplo Estados Unidos o la Unión Europea recibe un ataque cibernético, o tantos otros casos que han sucedido este mismo año, llegan al conocimiento de los ciudadanos porque se hacen públicos. Sin embargo, en otros países no se conocen casos. ¿Es esto debido a que no sufren ataques? En absoluto, normalmente se debe al oscurantismo informativo. Y China, por una vez, se ha abierto y en agosto confesó que el año pasado recibió 500.000 ataques, la mayoría de ellos con procedencia de países extranjeros

En **septiembre** conocimos que la empresa japonesa Mitsubishi Heavy Industries fue atacada. Casi 100 ordenadores habían sido infectados, aunque la empresa dijo que ninguna información confidencial había sido robada. Esta empresa fabrica material muy delicado, como misiles guiados, motores de cohetes y equipamiento para centrales nucleares. Tras las primeras investigaciones se descubrió que los atacantes habían utilizado herramientas de software en chino, por lo que de nuevo las miradas se dirigieron al gigante asiático. Y los peores temores vinieron después, cuando se confirmó que sí habían tenido acceso a información confidencial, tanto de motores de aviones y helicópteros de combate como de diseño de plantas de energía nuclear.

En **octubre** se hizo público que varios UAV (vehículo aéreo no tripulado) utilizados por Estados Unidos habían sido víctimas de una infección. Tras las primeras sospechas sobre si era un ataque dirigido con algún tipo de intención bélica, se supo que había sido una "accidente" debido a que los UAV se actualizan mediante llaves USB, y algunas de éstas estaban infectadas.

En **diciembre**, el gobierno iraní hizo pública la foto de un UAV norteamericano que habían capturado en perfecto estado. Lo llamativo de este caso es que habían conseguido hackear la señal del GPS del aparato para que aterrizara en su territorio, mientras el aparato creía que estaba de vuelta en su base.

FIG.08. *UAV NORTEAMERICANO CAPTURADO POR IRÁN TRAS HACKEARLO EN PLENO VUELO.*

STUXNET

Este ha sido el mayor ataque de ciberguerra conocido registrado hasta la fecha, descubierto en 2010 y cuyo objetivo era sabotear el programa nuclear del gobierno de Irán. En 2011 supimos que detrás del ataque estaba Israel, al conocer una noticia que nos sorprendió a todos cuando el General israelí Gabi Ashkenazi, en una fiesta celebrando su último día de trabajo, se atribuyó el ataque de Stuxnet como uno de sus triunfos.

También este año la web DEBKAfile publicó un informe citando "fuentes de inteligencia" en el que se afirmaba que Irán había tenido que sustituir miles de centrifugadoras de uranio debido al ataque sufrido el año pasado, y que desde entonces no han conseguido volver a enriquecer uranio al ritmo normal. El gobierno iraní, de hecho, confirmó a través de su ministro de asuntos exteriores que está instalando "nuevas y más rápidas" centrifugadoras para acelerar el proceso de enriquecimiento de uranio.

En julio, el Departamento de Interior norteamericano, refiriéndose al caso Stuxnet, dijo al Congreso que temen que el mismo tipo de ataque pueda ser utilizado contra infraestructuras críticas de su país. El hecho de que cada vez haya disponible más información hace temer que se creen variantes que puedan atacar a otro tipo de sistemas del país.

En 2011 hizo aparición Duqu, también conocido como "Stuxnet 2.0" o "el hijo de Stuxnet", que no es más que un troyano que reutiliza varias partes de Stuxnet para el robo de información. Se distribuyó a través de mensajes de correo dirigidos a víctimas específicas con documentos de Word adjuntos que tenían una vulnerabilidad 0-day (para la que no existía parche alguno).

Mac

En plataformas Mac hemos visto por primera vez un ataque a gran escala, protagonizada (¡cómo no!) por falsos antivirus. A pesar de que la instalación del falso antivirus (llamado MacDefender) afectó a miles de usuarios de todo el mundo, Apple trató de negar la evidencia. Días después cambió de opinión, y publicó una "actualización de seguridad" (sic) que protegía contra este malware. En cuestión de minutos comenzaron a aparecer nuevas variantes, como MacShield, que se saltaban esta actualización de Apple, algo lógico si vemos que se basa en tecnología que tiene más de 20 años y que hoy en día está claramente superada, siendo inservible a no ser que se combine con técnicas modernas como el análisis por comportamiento.

Además, hemos podido ver cómo los ciberdelincuentes van explorando nuevas técnicas que demuestran cómo su interés por esta plataforma va creciendo. Este mismo año apareció el primer troyano para Mac capaz de detectar si se estaba ejecutando en una máquina virtual. Esta es una técnica muy utilizada en malware basado en Windows para dificultar el análisis llevado a cabo por los laboratorios de investigación antimalware, y el hecho de haber aplicado la misma técnica en malware diseñado para Mac demuestra que esta plataforma está en el punto de mira de estos ciberdelincuentes.

Malware en Móviles

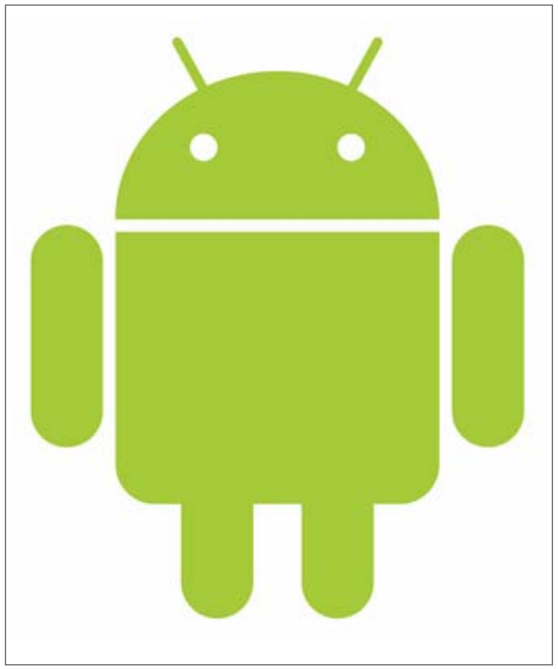
Este año 2011 los titulares hablando de malware para dispositivos móviles han sido unos de los protagonistas. Android se está convirtiendo en la plataforma de referencia en telefonía móvil, y es posible que muy pronto lo sea en el terreno de las tablets.

Los ciberdelincuentes están empezando a percatarse de que hay un incipiente mercado del que se pueden beneficiar, y están comenzando a realizar pruebas sobre el mismo, al mismo tiempo que siguen con técnicas que ya habían probado con éxito en el pasado, utilizando malware para enviar SMS a números premium.

A comienzos de año detectamos un nuevo malware para Android que aparecía en escena, se trataba de un troyano –detectado como Trj/ADRD.A- que robaba información personal y la enviaba al delincuente. Una de las recomendaciones que más se repetían al hacerse eco de esta noticia, era la de no descargarse aplicaciones de tiendas alternativas o de lugares cuya procedencia no sea fiable. En esta ocasión, el troyano había sido distribuido en tiendas de Android en China (no en la oficial) junto a juegos y fondos de pantalla.

A diferencia que con el iOS en el iPhone, en Android puedes instalar cualquier aplicación desde cualquier lugar, algo que los delincuentes están empezando a explotar. Pero esta no es la única diferencia, ya que las aplicaciones que se suben a la tienda oficial de Android (Android Market) tampoco son examinadas con la misma minuciosidad que las de Apple, lo que ha dado lugar a algún que otro "susto".

Unos días más tarde tuvo lugar la distribución de otro troyano para Android, también en China, que venía oculto dentro de una aplicación legal que los ciberdelincuentes habían reempaquetado con el troyano de regalo. Este troyano tenía diferentes funcionalidades, desde el envío de SMS a visita de páginas web. También permitía bloquear SMS entrantes.



A principios de marzo tuvo lugar el mayor ataque de malware en Android conocido hasta la fecha, esta vez las aplicaciones maliciosas se encontraban el Android Market, la tienda oficial para comprar aplicaciones. En sólo 4 días las aplicaciones que instalaban el troyano habían tenido más de 50.000 descargas. El troyano en esta ocasión era mucho más avanzado, ya que no sólo robaba información personal del dispositivo, sino que podía descargar e instalar otras aplicaciones sin el conocimiento del usuario.

FIG.09. ***ANDROID SE HA CONVERTIDO EN EL SISTEMA OPERATIVO MÓVIL PREFERIDO POR LOS CIBERDELINCUENTES.***

Google eliminó todas las aplicaciones maliciosas de su tienda, y días más tarde eliminó las aplicaciones maliciosas de los móviles de los usuarios.

Otro gran ataque a dispositivos móviles tuvo lugar también a principios de año, esta vez de manos de los creadores del famoso troyano bancario conocido como ZeuS. Como muchos bancos están comenzando a utilizar un doble factor de autenticación utilizando dispositivos móviles, cuando nuestro PC está infectado y vamos a hacer alguna transacción nos aparece en la página del banco (modificada por el troyano Zeus) una pantalla donde nos solicitan el nº de móvil y el modelo, de tal forma que nos enviarán un mensaje para instalar un "certificado de seguridad" en el móvil, que es realmente un troyano preparado para interceptar todos los mensajes que recibamos.

Por si esto no fuera suficiente hemos conocido que Android tiene algunos fallos de seguridad muy básicos, como demuestra el hecho de que almacena las contraseñas de correo electrónico en el dispositivo sin ningún tipo de encriptación, en texto plano. Esto facilita la vida a los ciberdelincuentes, ya que de una forma sencilla podrían robar todas las credenciales una vez han conseguido acceso al dispositivo.

La aparición de nueva familias de malware para Android es algo cada vez más frecuente, cada una con diferentes objetivos aunque todas comparten uno en común: el robo de información. Así, hemos visto malware que no sólo copia datos del terminal y los envía a los ciberdelincuentes, sino que es capaz de grabar las conversaciones que tengamos en el teléfono móvil.

En total, Google ha eliminado más de 100 aplicaciones maliciosas a lo largo de 2011, lo que puede ser un golpe a la confianza de los usuarios que confían en el fabricante de su sistema operativo para filtrar las aplicaciones maliciosas antes de subirlas al Market.

Ciberactivismo

Ya en 2010 augurábamos que el ciberactivismo iba a ser un protagonista indiscutible a lo largo del año entrante, y efectivamente así ha sido.

En Egipto Internet se convirtió en una especie de campo de batalla entre el gobierno egipcio y los protestantes, principalmente en lugares como Facebook o en páginas de grupos como Anonymous.

El gobierno egipcio llegó a sentirse tan acorralado, que en una acción sin precedentes cortó completamente el acceso a Internet y las redes de telefonía móvil de todo el país.

Por otro lado, en diferentes países occidentales desde donde usuarios participaron en los ataques de 2010 en defensa de Wikileaks dentro de la conocida como "Operation: Payback", se han realizado detenciones de usuarios que participaron en los mismos.

FIG.10. *CARTEL DEL GRUPO ANONYMOUS ANUNCIANDO SU CAMPAÑA A FAVOR DE LOS PROTESTANTES EGIPCIOS.*

Principalmente se trata de adolescentes que utilizaron la herramienta LOIC para participar en los ataques sin utilizan ningún tipo de proxy anónimo o red privada virtual que les hubiera permitido ser indetectables. Todo apunta a que se trata de una acción ejemplarizante por parte de los gobiernos (Holanda, Reino Unido y EEUU) para amedrentar a los protestantes.

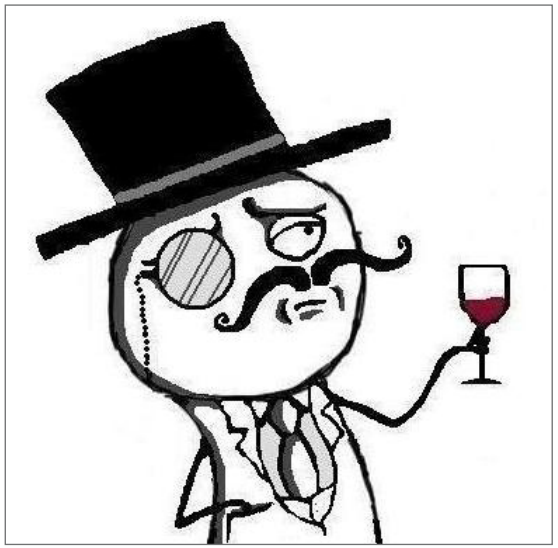
Otra "batalla" digna de mención ha sido la protagonizada por la firma de seguridad norteamericana HBGary Federal y el grupo Anonymous. Todo comenzó cuando el CEO de la compañía americana, Aaron Barr, dijo tener datos de los cabecillas de Anonymous y que pensaba hacerlos públicos. Simpatizantes de Anonymous se sintieron aludidos, por lo que ni cortos ni perezosos trataron de colarse en la compañía… y lo consiguieron en apenas unas horas. No sólo hackearon su página web y su cuenta de Twitter, sino que consiguieron robar decenas de miles de correos electrónicos que acto seguido fueron distribuidos desde The Pirate Bay.

Por si esto no fuera suficiente, el contenido de algunos de estos correos ha resultado ser realmente comprometedor para la compañía norteamericana, ya que han sacado a la luz prácticas claramente inmorales (como la propuesta de desarrollo de un rootkit) que han colocado a la empresa en una situación tan delicada que su CEO, Aaron Barr, no ha tenido más remedio que dimitir.

Y este caso de HBGary no fue más que el pistoletazo de salida para un cúmulo de despropósitos protagonizados por el grupo Anonymous, que parece que para protestar tiene que llevar a cabo actos ilegales. Como ya dijimos en informes anteriores, el hecho de que sus protestas supongan violaciones de la legalidad hace que sus denuncias pierdan legitimidad. Durante los últimos meses han perpetrado ataques contra la web de la Cámara de Comercio de Estados Unidos, Sony, la Policía Nacional española, webs de diferentes gobiernos y un largo etcétera.

Además se justifican publicando comunicados en los que indican que sus actos son "protestas pacíficas", a pesar de las pérdidas económicas que causan y las ilegalidades que cometen. Dicen representar y ser la voz de "el pueblo", a pesar de lo cual no son capaces de dar la cara, escondiéndose tras seudónimos.

Además de Anonymous, apareció otro grupo autodenominado LulzSec, que opina que el vandalismo y la delincuencia es algo divertido (sic).



Su principal método de "trabajo" ha sido robar bases de datos de diferentes empresas (PBS, Fox, etc.) además de alguna denegación de servicio (como el llevado a cabo a la página web de la CIA). Por si esto no fuera suficiente, han publicado los datos personales de usuarios que previamente habían robado, incluyendo direcciones de correo, contraseñas, etc. lo que ha facilitado que se realicen todo tipo de secuestros de cuentas y robos.

FIG.11. *IMAGEN DE PERFIL UTILIZADA POR LULZSEC EN SU PERFIL DE TWITTER.*

A finales de junio, LulzSec y Anonymous lanzaron una operación conjunta llamada "Operation: Anti-Security" con el objetivo de atacar a páginas de cualquier gobierno o entidad gubernamental que se cruce en su camino.

Pero no todo son malas noticias, ya que se han producido varios arrestos de miembros de Anonymous en todo el mundo a lo largo de 2011.

En Estados Unidos Anonymous fue un paso más allá entrando en la empresa Booz Allen Hamilton (contratista del Departamento de Defensa –DoD) y robando 90,000 direcciones de correo militares y sus respectivas contraseñas. Consiguieron entrar a través de un servidor que se encontraba completamente desactualizado y desprotegido, ni siquiera contaba con protección antivirus.

Todos estos ataques no quedan sin respuesta, y el FBI detuvo en Estados Unidos a 16 personas relacionadas con Anonymous, enfrentándose a penas de entre 5 y 10 años de cárcel si son declarados culpables.

En cualquier caso ninguna de estas acciones ha conseguido parar a Anonymous, y según pasa el tiempo hemos visto cómo ha ido a más. Días después de estos arrestos Anonymous publicó un documento confidencial de la OTAN. Confirmó que tenía 1 Gb de datos más que no iba a publicar porque sería "irresponsable".

Mientras, en Italia Anonymous robó más de 8 Gb de datos del CNAIPIC (centro nacional contra el crimen informático para la protección de infraestructuras críticas).

FIG.12. *MENSAJE DE ANONYMOUS VANAGLORIÁNDOSE DE SU ÚLTIMO ROBO DE DATOS.*

Además, robaron y publicaron miles de datos de policías norteamericanos, incluyendo sus direcciones de correo, nombres de usuario, contraseñas y en algunos casos hasta su número de la seguridad social. Semanas más tarde repitieron la operación, en este caso dirigida a policías del metro de San Francisco. Por si no fuera suficiente, volvieron a atacar a una empresa contratista del DoD (Vanguard Defense Industries) robando 1 Gb de datos con correos electrónicos y documentos privados pertenecientes a uno de los ejecutivos de la compañía.

Para despedir el año, Anonymous robó miles de números de tarjetas de crédito de clientes del think tank Stratfor, y las utilizó para realizar donativos a diferentes organizaciones. Asimismo publicó parte de la información robada, que en total ocupa 200 Gb. Por si fuera poco, dentro de esta lista de clientes podemos encontrar a empresas como Apple o la mismísima Fuerza Aérea norteamericana.

03| El 2011 en cifras

26.000.000 de nuevas muestras de malware han sido recogidas a lo largo del año 2011, unas 73.000 nuevas muestras diarias, una cifra escalofriante, la más alta en toda la historia. Este podría ser el resumen de cifras, aunque merece la pena bucear un poco y ver exactamente qué está sucediendo. Para empezar, conviene echar un vistazo a qué tipo de malware ha sido creado durante los últimos 12 meses:

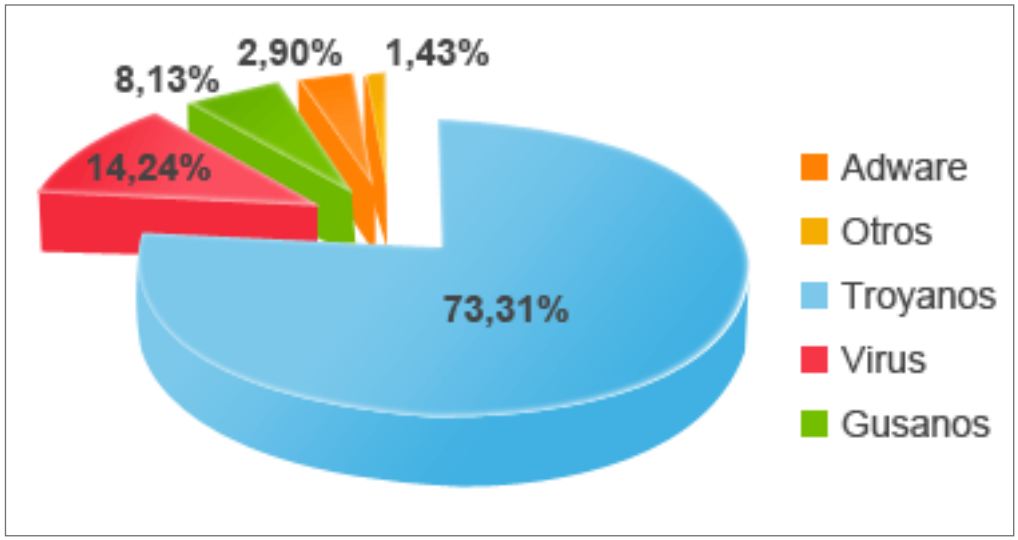


FIG.12. *NUEVO MALWARE CREADO EN 2011, POR TIPO.*

El tipo de malware dominante sigue siendo el troyano, aunque cabe destacar el espectacular crecimiento que ha tenido. En 2009 el porcentaje de troyanos era del 60%, en 2010 bajó al 56% y este año pasado ha pegado un salto hasta el 73%, casi 3 de cada 4 nuevas muestras de malware creadas durante 2011 han sido troyanos. El resto de categorías pierden relevancia

respecto a esta categoría reina, la favorita de los ciberdelincuentes para llevar a cabo intrusiones y robos de información.

Otra perspectiva desde la que podemos analizar los datos son las infecciones causadas por cada categoría. Una de las características de los troyanos es que no se replica, por lo que su capacidad teórica de infección es mucho menor en comparación a virus o gusanos, que pueden infectar por sí mismos gran cantidad de PCs. Veamos cómo se reparten las infecciones:

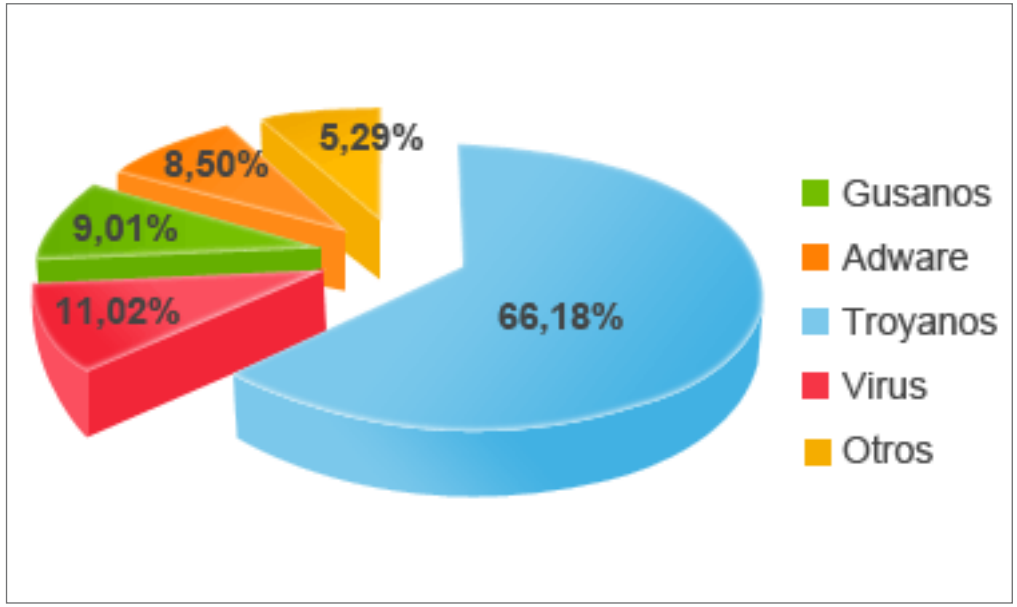


FIG.13. *INFECCIONES POR TIPO DE MALWARE EN 2011.*

Podemos observar cómo no hay tanta diferencia entre los tipos de malware creados y las infecciones que cada uno de ellos causa. Salvo por una excepción: vemos que en la categoría Adware/Spyware casi tripicla en porcentaje los PCs infectados respecto a los ejemplares creados.

¿Cuál es la explicación a esta "anomalía"? Resulta que en dicha categoría se engloban los falsos antivirus, también conocidos como rogueware, aplicaciones creadas por los ciberdelincuentes que se hacen pasar por antivirus o por otro tipo de utilidades que tratan de engañarnos mostrando falsa información sobre la seguridad de nuestro equipo, diciendo que está en grave riesgo, y pidiendo a continuación la compra de una licencia del software para poder solucionar los diferentes problemas mostrados.

Es un sistema ideal para los ciberdelincuentes, porque ni siquiera deben robar la información al usuario, ya que será este el que mediante engaños pague voluntariamente la cantidad de dinero solicitada. Por este motivo los ciberdelincuentes se preocupan de distribuir al mayor número de usuarios posible sus rogueware, a mayor número de infecciones lograrán un mayor beneficio económico.

Otro análisis que podemos realizar es el geográfico. ¿Qué países están más infectados? ¿Cuáles están mejor protegidos? La media de PCs infectados a nivel mundial es del 38,49%, pero nos encontramos con que el país más infectado del mundo en 2011 fue China, con un 60,57% de PCs infectados. Le siguen en el ranking Tailandia, con un 56,16% y Taiwan (52,82%). Cabe destacar que son los únicos países que sobrepasan el 50% de infecciones, a continuación podemos ver los 10 países con mayor índice de infección:

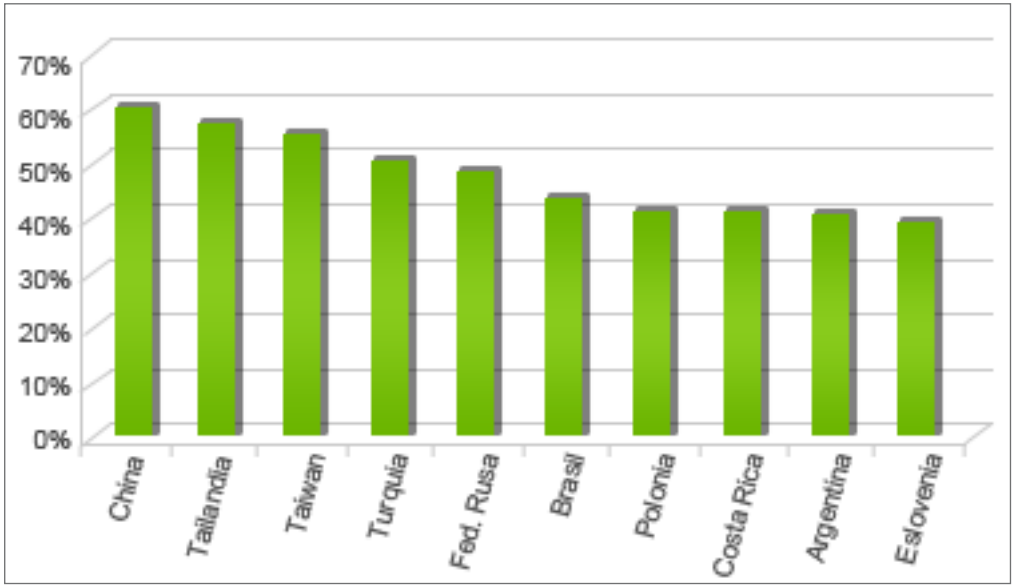


FIG.14. *PAÍSES CON MAYOR ÍNDICE DE INFECCIÓN.*

Vemos que los países más infectados están repartidos geográficamente. Estados Unidos se ha librado por poco de estar en este Top 10, ya que se encuentra en el puesto número 11 con un 39,02% de infecciones, también por encima de la media mundial.

Si vemos los datos de los países mejor posicionados, aquellos cuyo índice de infección es más bajo, vemos que excepto Australia y Japón el resto son europeos, siendo Suecia el que ostenta el lugar más alto del podio con un porcentaje que no llega al 25%:

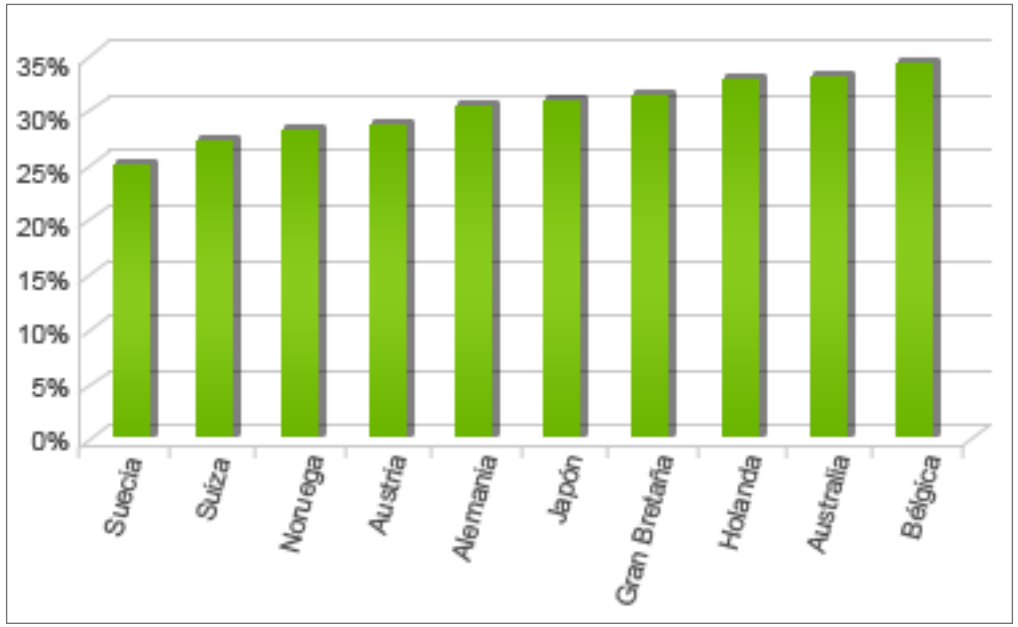


FIG.15. *PAÍSES CON MENOR ÍNDICE DE INFECCIÓN.*

04| Tendencias de Seguridad 2012

Hemos visto cómo ha transcurrido todo 2011: récord en creación de malware, en troyanos, ataques en redes sociales, ciberdelincuencia por doquier y ciberguerra en todo el mundo. ¿Qué podemos esperar para 2012?

Redes sociales

Los ataques de ingeniería social funcionan muy bien para engañar a los usuarios de redes sociales, y la utilización de temas populares como las próximas Olimpiadas o las elecciones a la presidencia de Estados Unidos serán un gancho que se utilizará. Las redes sociales también tendrán su importancia ya que cada vez hay más usuarios y se tratará de abusar de estas plataformas para tratar de infectar y sacar provecho de los ejemplares de malware, así como cualquier otra táctica para poder sacar un beneficio (spam, robo de información, etc.).

Crecimiento de malware

Durante los últimos años, el número de ejemplares de malware creados ha crecido de forma brutal, y todo indica que durante 2012 va a continuar esta tendencia. No en vano el malware es el armamento utilizado por los ciberdelincuentes para llevar a cabo sus ataques.

Troyanos

Los troyanos seguirán siendo el arma preferida por los ciberdelincuentes para llevar a cabo sus ataques. Durante 2011, 3 de cada 4 nuevos ejemplares de malware creados eran troyanos, la mayoría de ellos diseñados para permanecer de forma silenciosa en nuestro ordenador mientras nos roban toda nuestra información.

Ciberguerra

O quizás sería más adecuado calificarlo de ciberespionaje. 2011 ha sido el año de la historia en el que hemos visto más casos de intrusiones en gobiernos e instituciones de todo el mundo. Desde Nueva Zelanda a Canadá, pasando por Japón y el mismísimo Parlamento Europeo, han sucedido ataques cuya finalidad era la obtención de información. Vivimos en un mundo en el que toda la información se encuentra en formato digital, por lo que el James Bond de turno ya no necesita infiltrarse físicamente en unas instalaciones para robar información, sino que "sólo" le basta con tener ciertas habilidades para poder acceder a los secretos mejor guardados, y todo desde el sofá de su casa. 2012 será un año donde este tipo de ataques será aún más frecuente.

Malware para Mac

Mientras observamos cómo la cuota de mercado de Mac va creciendo, vemos también que el interés de los ciberdelincuentes en esta plataforma aumenta. Afortunadamente parece que los usuarios de Mac se van concienciando de que no viven en una plataforma inmune y el uso de antivirus en esta plataforma también ha aumentado, dificultando un poco más el trabajo a los ciberdelincuentes. Durante 2012 crecerá el número de ejemplares de malware para Mac, aunque aún estarán muy lejos de las cifras que existen en PC.

Malware para móviles

Hace más de una década ya podíamos encontrar compañías antivirus que nos vendían el apocalipsis en el mundo de los móviles, contándonos que íbamos a sufrir una inundación de ataques en estos dispositivos. Años más tarde, y a pesar de seguir prediciendo lo mismo, la situación no cambió, por lo que empezaron a utilizar el argumento de que no había sucedido gracias a los antivirus para móviles. Evidentemente volvían a estar equivocados; si por la existencia de antivirus se solucionaran los problemas de malware todos viviríamos mucho más tranquilos, pero lamentablemente no somos ni los usuarios ni los fabricantes de software de seguridad los que tomamos este tipo de decisiones, sino los ciberdelincuentes que atacan a las plataformas que más beneficio les pueden reportar. Ya en este contexto, para 2011 vaticinamos un aumento notable en la creación de malware para Android, vaticinio que ha sido confirmado, siendo Android el sistema operativo móvil más atacado durante este año. En 2012 continuarán los ataques a Android, y aumentarán, pero no en forma de epidemia. Sin embargo, a lo que debemos estar atentos es a los nuevos sistemas de pago mediante teléfono móvil que se van a comenzar a extender a lo largo de 2012, como los basados en el estándar NFC, que podrían motivar aún más a los ciberdelincuentes para diseñar troyanos que traten de atacarlos. Como todo, dependerá principalmente de la popularidad que dichos sistemas lleguen a alcanzar.

Malware para Tablets

Al compartir sistema operativo con sus hermanos pequeños, los smartphones, se verán igualmente afectados por el malware que aparezca para estas plataformas. Además, los tablets tienen un atractivo extra para los ciberdelincuentes, ya que muchos usuarios lo utilizan como un sustituto del PC y almacenan en el dispositivo información susceptible de ser robada de forma mucho más habitual que en los teléfonos.

Pequeñas y medianas empresas en el punto de mira de los ciberdelincuentes

¿Por qué los clientes de entidades financieras son atacados constantemente en lugar de atacar directamente a estas entidades para robar el dinero? La respuesta a esta pregunta es el análisis del coste-beneficio que se lleva a cabo: las entidades financieras suelen estar muy bien protegidas, por lo que conseguir llevar a cabo un ataque exitoso, además de poco probable es muy costoso, mientras que atacar a sus clientes para robar su identidad y hacerse pasar por ellos es algo mucho más sencillo. Sin embargo, si miramos a pequeñas y medianas empresas, su seguridad no es tan férrea, por lo que pasan a ser un gran atractivo para los amantes de lo ajeno, ya que de un solo golpe pueden llevarse información de cientos o miles de usuarios. En muchos caso las pequeñas y medianas empresas no cuentan con un equipo dedicado a la seguridad informática, lo que las hace mucho más vulnerables.

Windows 8

La nueva versión del popular sistema operativo de Microsoft será lanzada, si todo va según lo previsto, en Noviembre de 2012. Si bien este lanzamiento no creemos que repercutirá en corto plazo (2012) en la creación de malware, abrirá nuevas posibilidades a los ciberdelincuentes. En Windows 8 se podrán diseñar aplicaciones que puedan funcionar en Windows 8 tanto en PCs, como en Tablets y Smartphones, por lo que el desarrollo de aplicaciones maliciosas como las que hemos visto en Android podrán llegar a ser una realidad, aunque lo más probable es que esto sea algo que no veremos hasta 2013.

05| Conclusión

El año pasado finalizábamos nuestro informe comentando que la situación parecía grave y que el 2011 se presentaba interesante. Lamentablemente no nos hemos equivocado, y ha sido un año en el que los ciberataques y los robos de datos han sido protagonistas. No queremos ser agoreros, pero 2012 no se presenta mucho mejor. El ciberespionaje y los ataques a través de las redes sociales serán protagonistas de este año que acaba de comenzar.

Las ventajas de estar en un mucho más interconectado, con un uso de las redes sociales en aumento y la capacidad de poder comunicarse con gente de cualquier punto del planeta, también tiene algunas desventajas. Los enemigos de lo ajeno tienen muchas más víctimas a las que poder robar datos o infectar sus PCs con ejemplares de malware. Como hemos podido ver en estos últimos años, no es necesario ser un "cerebrito" para poder hacerse cargo de un PC, o modificar un código malicioso para crear nuevos ejemplares.

Cada vez somos más los usuarios de Internet, y en consecuencia, muchas más potenciales víctimas. Imaginaos una calle céntrica de cualquier gran ciudad en época de compras de navidad y a los típicos carteristas. Hay muchas más calles céntricas y grandes ciudades (más plataformas, redes sociales, móviles, tablets, etc.), y más posibilidades de dejar tu cartera expuesta para que los ciberdelincuentes se lleven tus tarjetas, las fotos de tus sobrinos y el dinero que lleves. Esta es la situación actual. Más víctimas para cada vez más carteristas.

A pesar de este panorama no debemos dejar de disfrutar de las ventajas que nos ofrece Internet, la banca online, hacer compras sin desplazarnos de nuestra casa, estar conectados con nuestros amigos de todo el mundo, poder leer un libro desde tu teléfono o tableta… Sólo es necesario que extrememos las precauciones. En definitiva, contar con un buen sistema de seguridad instalado y actualizado y realizar una navegación responsable son las claves para sentirse seguro en la Red.

06| Sobre PandaLabs

PandaLabs es el laboratorio antimalware de Panda Security, y representa el centro neurálgico de la compañía en cuanto a tratamiento del malware se refiere:

- Desde **PandaLabs** se elaboran en tiempo real y de forma ininterrumpida las contramedidas necesarias para proteger a los clientes de Panda Security de todo tipo de códigos maliciosos a escala mundial.

- **PandaLabs** se encarga asimismo de llevar a cabo el análisis detallado de todos los tipos de malware, con la finalidad de mejorar la protección ofrecida a los clientes de Panda Security, así como para informar al público en general.

Del mismo modo, **PandaLabs** mantiene un continuo estado de vigilancia, siguiendo muy de cerca las diferentes tendencias y evoluciones acontecidas en el campo del malware y la seguridad. Su objetivo es avisar y alertar sobre inminentes peligros y amenazas, así como formular previsiones de cara al futuro.

- Se puede obtener información sobre las últimas amenazas descubiertas por en el blog de **PandaLabs** en: **http://pandalabs.pandasecurity.com/**

Síguenos en la Red

facebook
https://www.facebook.com/PandaSecurity

twitter
https://twitter.com/PandaComunica

google+
http://www.gplus.to/pandasecurityes

youtube
http://www.youtube.com/pandasecurity1

PANDA SECURITY