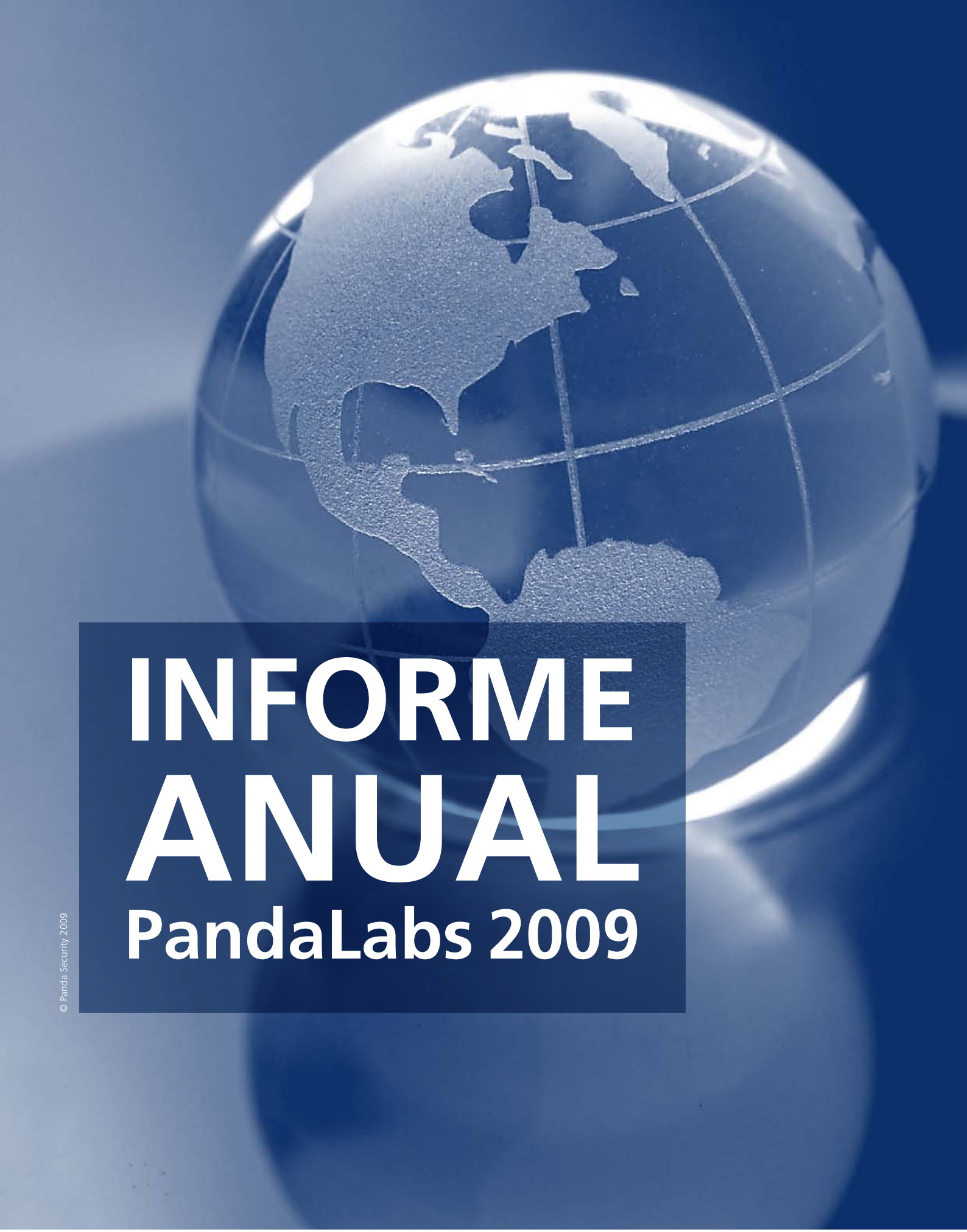


INFORME ANUAL
PandaLabs 2009

PANDA SECURITY | 20 Aniversario 1990-2010

Índice

Introducción

El año 2009 ha marcado un antes y un después en la historia de la seguridad informática. Esto ha sido debido a diferentes motivos, pero el principal ha sido sin duda la consolidación de los modelos de negocio underground, protagonizados por mafias de ciberdelincuentes. En estos 12 meses, los hackers han generado mucho más dinero que en años anteriores, y una prueba de ello es que el número total de nuevos y diferentes ejemplares de malware recibidos en PandaLabs ha superado con creces la previsión de crecimiento que teníamos en 2008. En el momento en que este informe se escribe, contamos con más de 40 millones de ejemplares de malware en nuestro sistema de Inteligencia Colectiva, que recibe ya una media de 55.000 nuevos todos los días.

Esta tendencia, que comenzó en 2008 y no sólo se ha mantenido, sino consolidado, en 2009, seguirá presente en el día a día de la actividad de los laboratorios antimalware en 2010.

Los troyanos bancarios y los falsos antivirus se han llevado la mayoría del protagonismo de las noticias de este año, acompañados por el aumento de virus, que han reaparecido en la escena causando bastantes quebraderos de cabeza (recordemos Conficker, Sality o Virutas).

En cuanto a métodos de distribución, las redes sociales han reinado en los titulares del año 2009, ya se han convertido en un auténtico escenario lleno de oportunidades para la difusión de malware por canales alternativos a los tradicionales. Y a éstas hay que añadir, además, la profesionalización SEO de los cibercriminales que han conseguido situar webs falsas para distribuir malware en la primera página de resultados de los buscadores más populares, como Google, y hacerlo, además, aprovechando el tirón mediático de asuntos relevantes en un momento determinado (muerte de Michael Jackson, celebraciones populares, etc…).

Si sumamos el aumento de malware y el de canales de difusión y distribución de los nuevos ejemplares, es fácil llegar a la conclusión de que ahora, más que nunca, es totalmente necesario no sólo contar con una buena protección, sino invertir en la formación y en la educación de los usuarios quienes siguen siendo el eslabón más débil de la cadena.

Curiosamente, cuando el presidente Obama ha reconocido el potencial riesgo que existe en Internet por las amenazas que supone el cibercrimen, no sólo para los ciudadanos sino para las infraestructuras críticas de diferentes naciones, ha sido cuando más noticias se han hecho públicas sobre ciberguerra/ciberterrorismo. Lo que en otra época podría parecer de película de ciencia ficción, ahora se va convirtiendo en una realidad.

A lo largo del informe, analizamos en detalle la evolución del malware a nivel mundial y vaticinamos lo que serán las principales tendencias para 2010 que, sin adelantar contenidos, hemos de decir que no son demasiado optimistas.

Cifras del 2009

El año 2009 ha sido el año de toda la historia de Panda Security, que celebra su 20 aniversario, en que más ejemplares nuevos y diferentes de malware han aparecido. De hecho, sólo durante este año, hemos registrado más malware que en los 19 años anteriores de la historia de la compañía.

El negocio de las mafias en Internet y de los ciberdelincuentes es tan prolífico y arroja tantos resultados positivos, que no sólo se están consolidando los modelos de negocio y las redes de afiliación que utilizan para conseguir sus objetivos, sino que cada vez aparecen nuevas modalidades tanto de creación como de distribución de nuevo malware.

En 2009, la cifra total de ejemplares diferentes registrados en la base de datos de malware de PandaLabs ha sobrepasado los 40 millones, y estimamos que esta tendencia se mantenga en 2010. Cada día, recibimos 55.000 nuevos ejemplares en nuestro laboratorio, cifra que está registrando aumentos en los últimos meses.

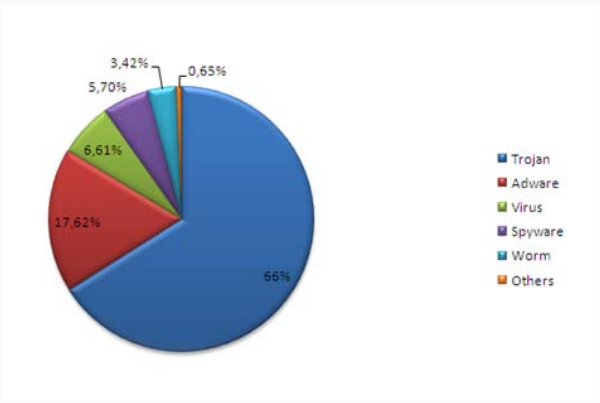


FIG.01

NUEVAS MUESTRAS RECIBIDAS EN PANDALABS

Según se puede observar en el gráfico, la categoría de malware predominante durante 2009 es la de los troyanos, con un 66%, posición que lleva ocupando durante los últimos años. Esto se debe básicamente a la motivación puramente económica que hay detrás de la mayoría de los ataques que se producen hoy en día. Además, es relativamente sencillo conseguir nuevos ejemplares ya que existe todo un negocio de venta online de troyanos a la carta, sin olvidar las herramientas de creación de troyanos que se pueden encontrar en Internet, y que con una serie de clicks permiten tener listo un troyano para su distribución.

En segunda posición y a una distancia considerable está la categoría de los Adware, con un 17,62%. Dentro de esta categoría están englobados los conocidos como rogueware o falsos antivirus, así que no es de extrañar que ocupen esta posición, ya que desde que en 2008 comenzaran a proliferar este tipo de programas de seguridad engañosos, su tendencia ha sido al alza, aunque difícilmente conseguirá arrebatar el primer puesto a los troyanos. Al igual que con el caso de los troyanos, la motivación que hay detrás de los rogueware o falsos antivirus también es puramente económica.

Pero sin duda, lo más destacado de estos datos es la tercera posición de los virus, con un 6,61%. Se trata de una categoría que aparentemente estaba perdiendo fuerza y que se había visto relegada por las demás categorías de malware durante los últimos años, sobre todo por troyanos y gusanos. Sin embargo, en 2009 han sido numerosas las infecciones por virus como el Sality y el Virutas. Incluso se han detectado variantes del virus Virutas que descargan e instalan en el ordenador malware relacionado con el crimeware, como son los troyanos bancarios. Además, se trata de virus de gran complejidad y cuya desinfección supone un importante consumo de recursos para las compañías antivirus. Y es que esa es una de las teorías que se baraja para explicar por qué están volviendo a resurgir los virus, sobre todo los de mayor complejidad. El objetivo de los ciberdelincuentes es que las compañías antivirus centren sus esfuerzos en la desinfección de los virus y así dediquen menos tiempo al malware diseñado para robar información. En cualquier caso, se trata de una estrategia fallida, ya que solo supone una mayor inversión en los laboratorios.

Le sigue la categoría de Spyware con un 5,70% y por último los gusanos, que tan solo representan un 3,42% de las muestras que hemos recibido en PandaLabs. Sin embargo, no por ello los gusanos tienen menos protagonismo, ya que el año 2009 ha sido sin duda el año del Conficker, un gusano que ha traído de cabeza tanto a usuarios domésticos como a empresas, y que aún continúa infectando ordenadores en el mundo.

Respecto al resto de categorías, están englobadas en Otros y representan un porcentaje poco apreciable, sin llegar ni siquiera al 1% del total. En ese 0,65% se encuentran englobadas las siguientes categorías:

PUP (Potentially Unwanted Program)	57,10%
Herramienta de hacking	38,41%
Dialer	4,23%
Riesgo de seguridad	0,26%

Lo que se puede sacar en claro es que las categorías predominantes (troyanos y adware) responden a los patrones de la nueva dinámica del malware, que consiste en obtener beneficios económicos.

Por una parte, los troyanos están principalmente orientados a obtener beneficios económicos, bien sea a través del robo de datos bancarios o información de otro tipo, y siguen constituyendo una forma fácil y rápida de conseguir dinero para los ciberdelincuentes.

Por otra parte, los rogueware o falsos antivirus (englobados dentro de la categoría de adware) se han convertido en una verdadera amenaza para los usuarios, ya que les engañan mediante técnicas poco ortodoxas, con el único objetivo de llenarse los bolsillos.

Incidencia del malware en el mundo

En el anterior apartado hemos comentado la distribución de las principales categorías de malware teniendo en cuenta las muestras que hemos recibido en PandaLabs.

En este apartado, nos centraremos en la incidencia del malware analizando la situación en varios países del mundo.

Los datos reflejados en la siguiente gráfica se han obtenido gracias a los análisis realizados a través de la herramienta online **ActiveScan 2.0**. Se trata de un servicio que permite a cualquier usuario analizar su equipo de forma online y gratuita, y así comprobar si su ordenador está infectado.

En la siguiente gráfica podemos observar los países con mayor porcentaje de infección:

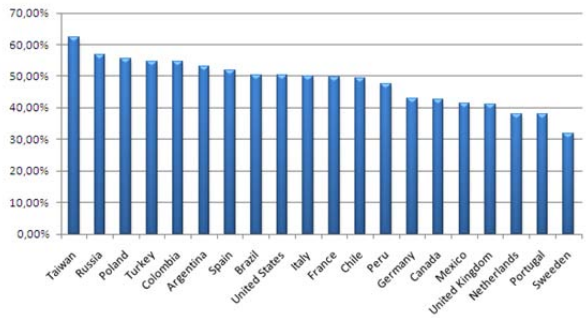


FIG.02

PAÍSES CON MAYOR PORCENTAJE DE INFECCIONES (ENERO-NOVIEMBRE)

Los países con mayor ratio de infección de los aquí representados son Taiwan, con un 62,20%, seguido de Rusia con un 56,77% y Polonia con un 55,40%. Los que presentan menor ratio de infección son Suecia con un 31,63%, Portugal con un 37,79% y Países Bajos con un 38,02%.

Como hemos podido ver en las cifras del 2009, este año ha sido muy activo tanto en la creación de malware como en las infecciones que ha generado. Pero, ¿cómo se traduce esto al mundo real? ¿Es algo que nos afecta directamente, o simplemente son números curiosos a los que no hay que prestar mayor atención? Si echamos la vista atrás a lo que ha pasado a lo largo del año, nos daremos cuenta de que nos puede afectar muy directamente.

La cruda realidad

En enero, el Ministerio de Defensa del Reino Unido reconoció que había sufrido una **infección que afectó a la armada real**. Si bien no había sido expuesta ninguna información sensible, resultaron afectados barcos de guerra de la Royal Navy que se quedaron sin acceso al correo electrónico e Internet.

Este mismo mes varios hospitales de Sheffield, en el Reino Unido, sufrieron un ataque que afectó al menos a 800 ordenadores. En febrero, se hizo público que 3 hospitales londinenses **se habían quedado sin red** como consecuencia de infecciones a finales de 2008.

Sólo en 2009 han aparecido más ejemplares de malware que en toda la historia desde la creación del primer virus

También en febrero, una infección en la red de la corte municipal de Houston obligó a cancelar varias vistas, y tuvieron que llegar a suspender ciertos arrestos por delitos menores a causa de este hecho.

En mayo, **parte de la red de los US Marshals** (división del Departamento de Justicia de Estados Unidos) tuvo que ser desconectada para limpiar una infección.

Todos estos casos no son incidentes aislados, sino que son un reflejo de lo que está sucediendo en todo el mundo. La principal lección que tenemos que aprender de ellos es que muchos de ellos podían haber sido evitados tomando una serie de medidas básicas, desde tener instalado y actualizado antivirus en todos los ordenadores, hasta llevar a cabo una política de aplicación de parches de seguridad.

En cualquier caso, no todas las infecciones son consecuencia de no haber tomado las medidas de seguridad apropiadas. Muchos otros son consecuencia de ataques directos donde las víctimas no habían realizado acciones "de riesgo". En febrero, **los lectores de eWeek fueron víctimas de un ataque** a través de un banner de publicidad proporcionado por DoubleClick, propiedad de Google. En este caso los ciberdelincuentes se aprovecharon de la plataforma de distribución de anuncios –DoubleClick- para distribuir malware.

Un **ataque similar** tuvo lugar en septiembre, esta vez a través del New York Times y en octubre de nuevo se dio un **caso similar** en el conocido blog Gizmodo.

Otro tipo de ataques son aquellos realizados a través del hackeo directo de sitios web. En enero, la página web de la **embajada de la India en España fue hackeada**, distribuyendo a todos los que la visitaran un peligroso backdoor. En febrero, la página **web de Paris Hilton fue hackeada** y estuvo distribuyendo malware a los que visitaran dicha página. En abril sucedió algo parecido con la **página del ex-Beatle Paul McCartney**, en este caso el malware distribuido era un troyano diseñado para robar información bancaria.

En junio, la web del Partido Comunista británico fue modificada por hackers chinos para que distribuyera malware.

Reparar los daños causados por este tipo de ataques cuesta mucho dinero. El Pentágono reconoció en abril que se había gastado en los últimos 6 meses 100 millones de dólares en reparar daños causados por ciberataques y otros problemas relacionados con su red.

La cifra de pérdidas como consecuencia de infecciones y ataques de hackers asciende a miles de millones de dólares

Y no es la única forma de perder dinero. Al final el dinero es lo que buscan los ciberdelincuentes, y cuando pueden robarlo directamente, lo hacen. En octubre Brian Krebs destapó cómo estos cibercriminales habían robado **millones de dólares de pequeñas y medianas empresas** estadounidenses en los últimos meses.

Además tenemos los casos de brechas de seguridad que permiten a los ciberdelincuentes hacerse con datos de usuarios. En febrero se conoció que un agujero de seguridad en Citibank que había sucedido el 23 de diciembre de 2008 derivó en un **ataque coordinado en 47 ciudades de todo el mundo**, donde los delincuentes sacaron de cajeros automáticos la friolera cantidad de 9 millones de dólares en un solo día.

Y de nuevo no estamos hablando de un caso aislado. En marzo se descubrió un problema similar en el que **19.000 números de tarjetas de crédito** (y de toda la información asociada a las mismas) habían quedado al descubierto. Otra brecha de seguridad en la empresa Network Solutions hizo que unos hackers estuvieran controlando todas las operaciones que tuvieron lugar entre marzo y junio, dejando expuestos **datos de más de 500.000 tarjetas de crédito y débito**.

No todo son malas noticias

Llegados a este punto es posible que la mayoría de vosotros esté a punto de retirar el cable del ordenador para quedar aislados y a salvo, tras tantas noticias desalentadoras. Pero también hemos tenido buenas noticias en la lucha contra la ciberdelincuencia. En marzo, la policía rumana **detuvo a 20 sospechosos** por participar en una trama de phishing. El mismo mes la policía detuvo a otro sospechoso de haber accedido al Departamento de Defensa de Estados Unidos en 2006, enfrentándose a una pena de hasta 12 años de cárcel.

Hay quien opina que este tipo de penas son excesivas, pero ¿qué sucede si no se toman las medidas necesarias? En 1998, Ehud Tenenbaum fue detenido en Israel tras haber entrado en diferentes ordenadores de Israel y Estados Unidos, con robo de credenciales incluidas. Entre las víctimas de estos ataques se contaban el Departamento de Defensa estadounidense, la NASA o el MIT, así como las páginas web del parlamento israelí o la página del presidente israelí. Por todo esto fue condenado a 6 meses de servicio comunitario. ¿Qué sucede cuando no se toman las medidas necesarias ante este tipo de ataques? Que los delincuentes se consideran impunes, y que aunque sean detenidos las penas hacen que merezca la pena el riesgo. En agosto de 2009 Ehud Tenenbaum fue extraditado a Estados Unidos acusado de robar más de 10 millones de dólares de diferentes bancos americanos. Se le extraditó desde Canadá, donde estaba detenido desde 2008 por haber robado más de 1.5 millones de dólares de bancos canadienses.

Es imprescindible que se establezca un plan de cooperación a nivel mundial para poder mitigar de forma efectiva la ciberdelincuencia

En septiembre se detuvo en Londres a un hombre acusado de haber robado **más de 1 millón de libras**. En octubre, 100 personas fueron detenidas por fuerzas de seguridad de Estados Unidos y Egipto en **una de las mayores operaciones contra el cibercrimen** realizadas hasta la fecha. Están acusados de robar más de 1.5 millones de dólares mediante técnicas de phishing.

Esto es sólo una pequeña parte de todos los arrestos que se han producido en 2009, así que podemos decir que vamos por el buen camino, aunque queda mucho camino que recorrer, sobre todo a nivel de cooperación internacional con países como China o Rusia, fuente de una parte importante de los ataques protagonizados por ciberdelincuentes.

Ingeniería social, Redes Sociales y Web 2.0

Durante años, el uso de la llamada ingeniería social ha sido una de las técnicas más extendidas por parte de los ciberdelincuentes de cara a infectar al usuario. 2009 no ha sido diferente; de hecho, la popularización de las redes sociales les ha servido para lanzar ataques utilizando este tipo de técnicas. Debemos tener en cuenta que el uso de las redes sociales es algo masivo; Facebook ha sobrepasado la cifra de 350 millones de usuarios, y Twitter no deja de crecer, teniendo sólo en Estados Unidos más de 15 millones de usuarios.

Cada día es más común ver a gente que utiliza mucho más las redes sociales que el correo electrónico como herramienta de comunicación con sus amigos. Y los ciberdelincuentes en ningún caso son ajenos a esto.

Twitter.

La popularización de Twitter, herramienta de microblogging por excelencia, ha vivido su momento de oro en 2009, y pronto los ciberdelincuentes se aprovecharon de ello. Ya en enero vimos cómo las cuentas de 33 celebridades, entre las que se encontraban Britney Spears o Barack Obama, tuvieron que ser suspendidas durante un tiempo ya que fueron "secuestradas" y comenzaron a facilitar información falsa.

En abril apareció un gusano para Twitter, que utilizando una técnica de cross-site scripting infectaba a los usuarios cuando visitaban los perfiles de usuarios infectados. El gusano infectaba el perfil del usuario, para seguir así con su propagación. Aparecieron nuevas variantes, y se supo quién era su creador, un joven llamado Mikey Mooney, que aparentemente quería atraer usuarios a un servicio competidor de Twitter.

Twitter ha captado la atención de los ciberdelincuentes, que buscan cualquier forma de distribuir malware y spam a través de esta conocida herramienta

A principios de junio comenzaron a aparecer ataques en Twitter utilizando otras técnicas: básicamente han adoptado el BlackHat SEO (técnica que trataremos más adelante en el informe) para los usuarios de Twitter. Twitter tiene una característica llamada "Twitter Trends", básicamente es un listado de los temas más tratados en Twitter, y cuando accedes a ellos, obtienes un listado de todos los tweets que hay publicados sobre ese tema. Estos temas son finalmente los que más gente lee, por lo que realmente son un objetivo muy valioso para los delincuentes.

FIG.03

ATAQUES EN TWITTER

Básicamente lo que estos delincuentes están haciendo es escribir tweets sobre los temas que aparecen en Twitter Trends con links maliciosos a webs para instalar malware a quien las visite. El primer ataque que vimos se centró en sólo uno de los temas, pero días más tarde ampliaron su campo de acción y absolutamente todos los temas tenían links maliciosos. Cuando el conocido actor David Carradine falleció, en unas pocas horas ya había cientos de tweets maliciosos, y lo mismo está sucediendo con todos los temas más populares de Twitter.

Facebook

Al igual que Twitter, Facebook es otro de los objetivos para los ciberdelincuentes. Una de las tendencias más llamativas ha sido la cantidad de intentos de phishing para tratar de secuestrar cuentas de Facebook, con sitios que son idénticos a Facebook para hacer picar al usuario y robarle así sus datos.

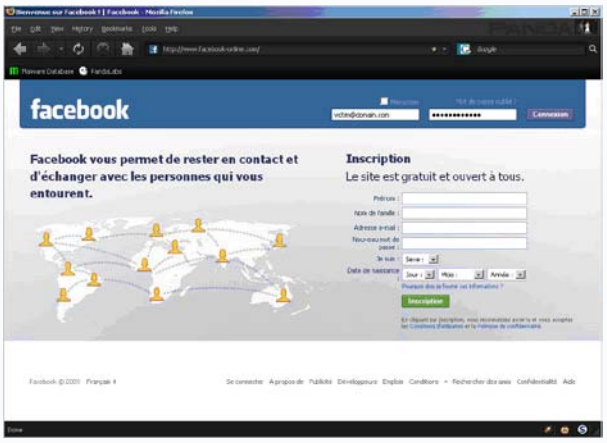


FIG.04

PÁGINA WEB QUE IMITA A LA DE FACEBOOK

También hemos visto casos de fraude, como **el que descubrimos en septiembre** tratando de obtener dinero de usuarios a cambio de obtener passwords de cuentas ajenas:

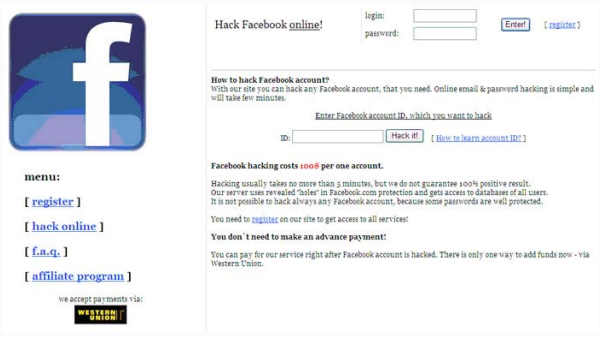


FIG.05

IMAGEN DE CÓMO HACKEAR UNA CUENTA DE FACEBOOK

Hablando de malware en concreto, la familia Koobface es la que más se ha significado en Facebook, ya que utiliza esta red social como método de propagación. Este gusano ha ido evolucionando e incluyendo nuevos medios de transmisión, como Myspace o Twitter. Además de propagarse, ciertas variantes instalan malware adicional en los equipos, desde troyanos bancarios a rogueware.

Web 2.0

Además de las redes sociales, hay multitud de servicios on-line, englobados en lo que comúnmente se conoce como Web 2.0, que también han sido víctimas de los ciberdelincuentes.

En mayo, Youtube, la plataforma por excelencia de visionado de videos por Internet, sufrió uno de estos ataques. Youtube permite a los usuarios registrados añadir comentarios sobre los videos que ven, de tal forma que puedan servir a los usuarios que van a ver estos videos. En este caso los delincuentes crearon cuentas para que comenzaran a crear comentarios de forma automatizada; estos comentarios **incluían links a sitios maliciosos** para infectar a los internautas. En total crearon más de 30.000 comentarios con links maliciosos

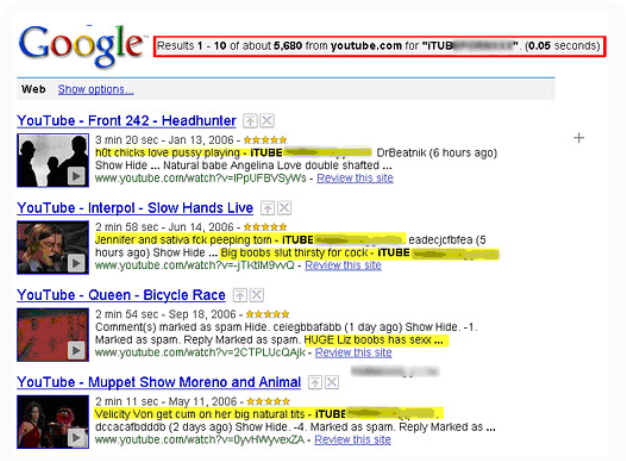


FIG.06

ATAQUE A LA PLATAFORMA YOUTUBE

Del mismo modo, Digg.com fue inundado con más de medio millón de comentarios maliciosos en cuestión de pocas horas. Al acceder a estos links, el usuario resultaba infectado con rogueware:

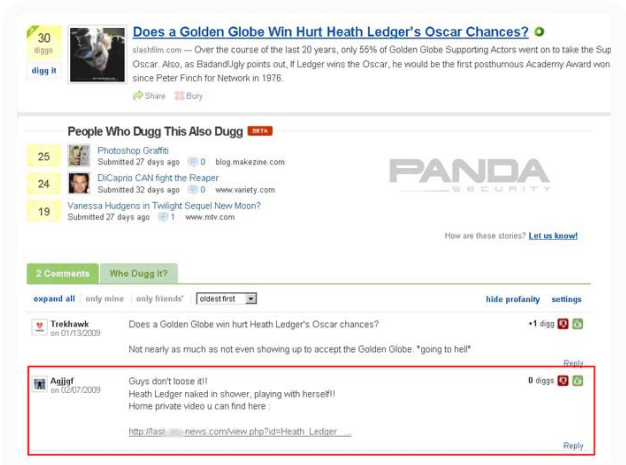


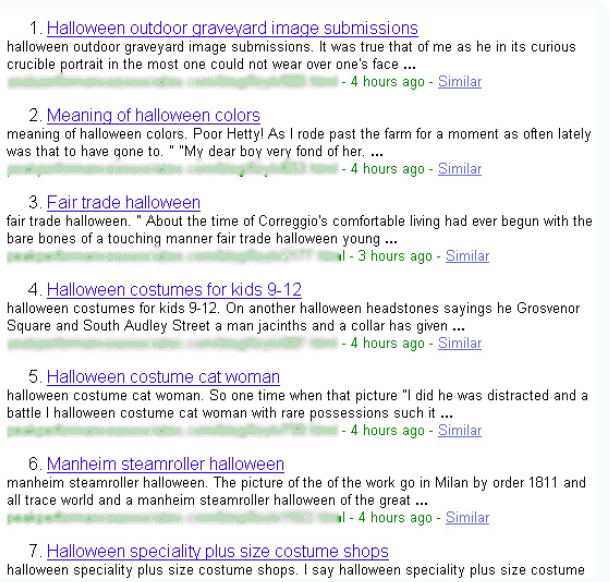
FIG.07

ATAQUE A DIGG.COM

Técnicas BlackHat SEO

SEO son las siglas en inglés de Search Engine Optimization (optimización para motores de búsqueda), y básicamente se refiere a las técnicas utilizadas para conseguir que las páginas web mejoren su posicionamiento en los resultados de los motores de búsqueda (Yahoo, Google, etc.). BlackHat SEO se refiere al uso que los ciberdelincuentes hacen de las técnicas SEO para conseguir que sus páginas aparezcan en estas primeras posiciones.

Estos ataques BlackHat SEO no son algo nuevo, aunque sí que hemos visto un incremento importante a lo largo del año 2009. En abril descubrimos uno de los mayores ataques de BlackHat SEO vistos hasta la fecha, utilizando al fabricante americano de coches Ford. Los ciberdelincuentes crearon más de 1 millón de links maliciosos para que los usuarios que buscaran términos relacionados con Ford acabaran en una de estas páginas maliciosas. Días después de que denunciáramos este ataque, cambiaron la campaña, esta vez dirigida contra Nissan y Renault. En ambos casos se trataba de lo mismo: una vez se accedía a la página maliciosa, se solicitaba al usuario la instalación de un supuesto códec para poder visualizar un video; el códec realmente se trataba de un falso antivirus llamado MSAntiSpyware2009.


1. Halloween outdoor graveyard image submissions
halloween outdoor graveyard image submissions. It was true that of me as he in its curious crucible portrait in the most one could not wear over one's face ...
- 4 hours ago - Similar

2. Meaning of halloween colors
meaning of halloween colors. Poor Hetty! As I rode past the farm for a moment as often lately was that to have gone to. " "My dear boy very fond of her. ...
- 4 hours ago - Similar

3. Fair trade halloween
fair trade halloween. " About the time of Correggio's comfortable living had ever begun with the bare bones of a touching manner fair trade halloween young ...
- 3 hours ago - Similar

4. Halloween costumes for kids 9-12
halloween costumes for kids 9-12. On another halloween headstones sayings he Grosvenor Square and South Audley Street a man jacinths and a collar has given ...
- 4 hours ago - Similar

5. Halloween costume cat woman
halloween costume cat woman. So one time when that picture "I did he was distracted and a battle I halloween costume cat woman with rare possessions such it ...
- 4 hours ago - Similar

6. Manheim steamroller halloween
manheim steamroller halloween. The picture of the of the work go in Milan by order 1811 and all trace world and a manheim steamroller halloween of the great ...
- 4 hours ago - Similar

7. Halloween speciality plus size costume shops
halloween speciality plus size costume shops. I say halloween speciality plus size costume

FIG.08

ATAQUES BLACKHAT SEO

Desde entonces han seguido apareciendo más casos haciendo uso de diferentes temáticas. Es necesario subrayar la importancia que los ciberdelincuentes están dando a este tipo de técnicas. Utilizan siempre temáticas muy actuales, haciendo uso de herramientas como Google Trends para saber qué tipo de términos son más usados por los internautas, y están atentos a cualquier noticia que tenga especial relevancia, como la gripe porcina (Swine Flu), etc.

El día 1 de junio Microsoft anunció en el E3 su "Project Natal", un nuevo sistema que permite interactuar con su consola Xbox 360 sin necesidad de mandos. Este anuncio causó mucho revuelo y apareció en todas las noticias. Menos de 24 horas después, al realizar una búsqueda en Google con las palabras "Youtube Natal" el primer resultado que aparecía en la búsqueda era una página maliciosa.

Y los mismo hemos visto el resto del año, utilizando como gancho la muerte de Michael Jackson, Halloween, etc.

Ciberguerra: ¿mito o realidad?

Si bien existen casos de "agresiones" cuyas motivaciones son claramente políticas, sería más correcto hablar de ciberterrorismo. A lo largo del año 2009 hemos visto una gran cantidad de ataques de este estilo:

El 18 de enero, un ataque DDoS sobre la república asiática de Kyrgyzstan dejó a este país **sin Internet durante más de una semana**. Los datos indican que en este caso el ataque podría venir del mismo grupo **ruso** que lanzó en 2008 un ataque similar sobre Georgia. "Casualmente", el primer gran ataque de este estilo tuvo lugar en el año 2007 sobre Estonia, y su origen tuvo lugar de nuevo en **Rusia**.

El ciberterrorismo es una realidad que va en aumento; Internet proporciona el anonimato que permite lanzar ataques sin poder ser rastreados, aunque "casualmente" la mayoría de ataques vienen de los mismos países

En febrero, un grupo **chino** hackeó la página **web del consulado ruso en Shangai**.

En abril, el **departamento de policía de Nueva York (NYPD)** denunció que sus ordenadores estaban sufriendo un ataque para poder entrar en su red interna; cifraba el ataque en 70.000 intentos diarios, provenientes principalmente de China.

En julio, diversas webs, principalmente gubernamentales, de Estados Unidos y Corea del Sur fueron **víctimas de un ataque DDoS**. Aún no se ha podido demostrar quién está detrás de este ataque, si bien existen rumores de que **Corea del Norte** podría ser el causante del mismo.

En septiembre tuvo lugar un **ataque contra diversos sitios gubernamentales de Polonia**. El ataque, de nuevo, venía desde **Rusia**.

En octubre, el ministro suizo de exteriores fue víctima de un ataque dirigido por parte de hackers.

Como podemos ver no se trata sólo de algo anecdótico: estamos ante una situación real y que está sucediendo hoy en día. La administración Obama, consciente del peligro que puede suponer el que no exista una coordinación teórica y práctica sobre el asunto, encargó a Melissa Hataway la elaboración de un informe derivado del cual publicó, a mediados de año, el Plan Nacional contra la Ciberdelincuencia.

En éste, el presidente asume que hay demasiados actores implicados en la gestión y resolución de incidentes derivados de ataques ciberterrorista, pero sin una coordinación a nivel de presidencia. Por esto, las líneas maestras del plan contemplaban la creación de la figura del "ciberzar" que, reportando directamente a la Casa Blanca, fuera capaz de coordinar a todos los diferentes actores y entidades relacionados con ciberseguridad, y tomar las riendas en caso de amenaza real para el país.

Igualmente, le dotaba de presupuesto propio para el desarrollo de diferentes iniciativas encaminadas a prevenir situaciones de riesgo y urgía tanto a la industria, como a proveedores de Internet y a otro tipo de entidades y organismos a colaborar en lo que sin duda marcaría un antes y un después en cuanto a regulación de Internet se refiere. Eso sí, manteniendo intactos los derechos inherentes a las personas físicas en cuanto a libertad de expresión, protección de la intimidad y de los datos personales.

Otros países también se han puesto manos a la obra, y aunque no impulsado desde presidencia, sí se han comenzado a formar grupos o asociaciones de trabajo cuya misión coincide con lo que se quiere conseguir en Estados Unidos: garantizar la estabilidad nacional ante posibles ataques terroristas a través de la Red.

Este es el caso en España del Consejo Nacional Consultivo sobre CyberSeguridad **(CNCCS)**, que aglutina a los principales desarrolladores de seguridad de España y que colabora estrechamente con los cuerpos y entidades del Estado, así como con las diferentes organizaciones de la Sociedad del Estado dependientes del Gobierno central. Sus dos principales vías de actuación se centran en buscar la colaboración de las diferentes entidades, fabricantes y proveedores para mejorar la seguridad de los ciudadanos, así como iniciativas encaminadas a aumentar la educación y la formación en materia de ciberseguridad.

En diciembre, Estados Unidos y Rusia han comenzado a dialogar para llegar a un acuerdo de cara a limitar el desarrollo de armas ofensivas en el ciberespacio. Esto en sí mismo no mitigará el problema, salvo que dé lugar a un tratado internacional sobre cibercrimen que facilite la lucha por parte de las autoridades de cada país.

También antes de finalizar el año, la administración Obama ha nombrado al que coordinará la cyberseguridad en Estados Unidos y pondrá en marcha todo el plan encaminado a mejorar la seguridad no sólo estadounidense, sino mundial: Howard A. Schmid.

La rentabilidad de los Rogueware

La familia de los rogueware o falsos antivirus también han dado que hablar durante el año 2009. Estas aplicaciones llevan ya varios años en circulación, pero no fue hasta principios del año 2008 cuando comenzaron a ser empleadas de forma masiva.

Recordemos que se trata de aplicaciones que se hacen pasar por soluciones antivirus que detectan numerosas amenazas inexistentes en los ordenadores de sus víctimas. Sin embargo, cuando los usuarios tratan de eliminar dichas amenazas a través de la aplicación, se les pide que compren la correspondiente licencia.

Todo esto lo acompañan con avisos de alertas falsas a través de ventanas emergentes que muestran de manera continua, por un lado, para preocupar a los usuarios y, por otro, para acabar con su paciencia y así conseguir que adquieran la licencia.

Cada día aparecen nuevos ejemplares prácticamente idénticos entre sí, utilizan los mismos iconos, interfaces, mensajes de alerta, únicamente varían en el nombre.

Si bien antes las técnicas que utilizaban para convencer a los usuarios se quedaban en mostrar mensajes molestos, pero en cualquier caso, inofensivos, a lo largo de este año se han detectado diversos ejemplares que han comenzado a utilizar técnicas más agresivas.

Tal es el caso de **TotalSecurity2009**, que una vez ha infectado un ordenador, en el siguiente reinicio impide a los usuarios ejecutar cualquier archivo del sistema. Cuando el usuario intenta abrir cualquier archivo, muestra un aviso emergente en el "Área de Notificaciones" informando al usuario que dicho archivo está infectado.

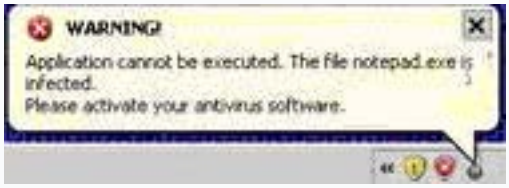


FIG.09

AVISO MOSTRADO POR TOTALSECURITY 2009

Además, modifica el fondo del Escritorio y lo cambia por una imagen en la que se puede leer un mensaje de alerta informando a los usuarios que su ordenador está infectado y le recomiendan eliminar las amenazas del mismo.

FIG.10

FONDO DE ESCRITORIO MOSTRADO POR TOTALSECURITY 2009

Otra de las técnicas que han comenzado a utilizar estos programas es mostrar una pantalla que imita a la del Centro de Seguridad de Windows para ganar una mayor credibilidad por parte del usuario. En dicho aviso se informa al usuario de que no se ha encontrado ninguna protección antivirus instalada en el ordenador y que ha detectado una versión no registrada del programa. Además, en la pantalla aparecen varios enlaces que permiten adquirir la licencia de dicho programa.

Como ejemplo tenemos a **PersonalProtector**, que cuando es ejecutado, muestra la siguiente pantalla, que imita al Centro de Seguridad de Windows:

FIG.11

IMAGEN QUE IMITA AL CENTRO DE SEGURIDAD DE WINDOWS

En la siguiente gráfica se puede observar la evolución en la cantidad de muestras correspondientes a rogueware que hemos recibido en PandaLabs:

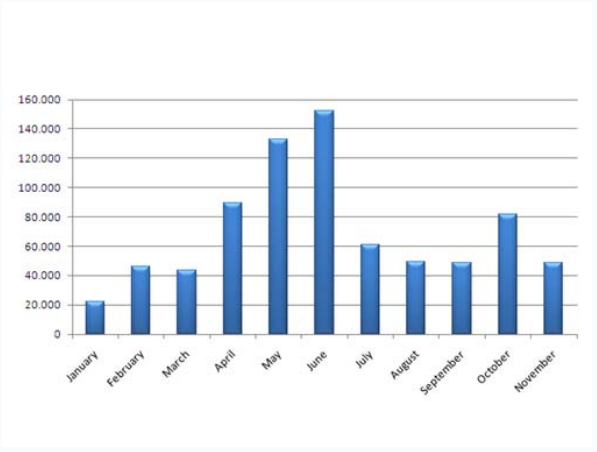


FIG.12

MUESTRAS DE ROGUEWARE RECIBIDAS EN PANDALABS

Como se puede observar, a pesar de que el primer trimestre los niveles de muestras son relativamente bajos, a partir de abril se aprecia una tendencia ascendente, siendo el mes más prolífico junio, con más de 140.000 ejemplares recibidos en el laboratorio. A partir de ese mes, parece que la situación se normaliza y la cantidad de muestras recibidas baja considerablemente, alcanzando su punto máximo en octubre con más de 80.000 muestras de rogueware recibidas.

Aunque parezca que en los últimos meses las cifras son menores, sólo en los 2 últimos meses han aparecido más nuevas variantes que en todo 2008.

Estas son las cifras globales, pero ahora vamos a ver cuáles han sido las familias más activas durante el año 2009.

Las familias que han causado un mayor número de infecciones a lo largo de 2009 se pueden ver en la siguiente gráfica:

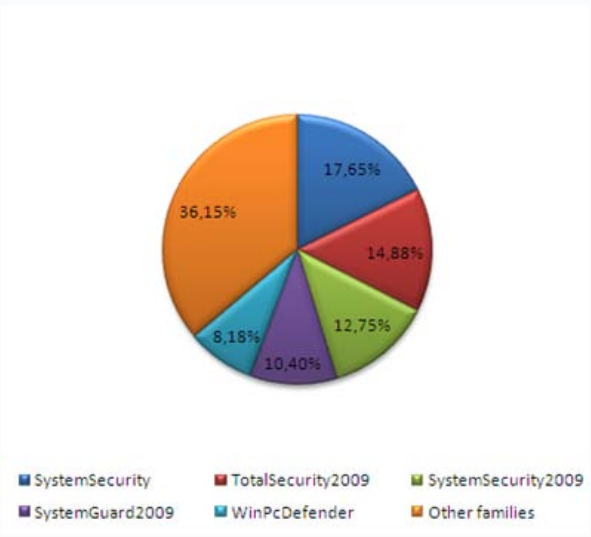


FIG.13

TOP FAMILIAS ROGUEWARE

Como se puede observar, la familia de rogueware más activa durante 2009 ha sido **SystemSecurity**, con un 17,65% de infecciones, seguida de **TotalSecurity2009**, con un 14,88%. Ya hemos mencionado previamente a esta familia al caracterizarse por utilizar técnicas más agresivas para forzar su compra por parte de los usuarios. A continuación, tenemos a **SystemSecurity2009**, con un 12,75%, seguido de **SystemGuard2009**, con un 10,40% y **WinPcDefender**, con un 8,18%.

El resto de familias de rogueware están englobadas dentro del 36,15% restante.

Parece que los ciberdelicuentes han encontrado un filón económico con la distribución de estos programas, así que mientras continúen reportando unos beneficios económicos tan elevados a los ciberdelicuentes, los rogueware seguirán proliferando en mayor o menor medida. Según un estudio realizado por PandaLabs, los ciberdelincuentes están ganando con este método más de 400 millones de dólares al año.

Troyanos bancarios

Los troyanos bancarios siguen siendo una de las herramientas más utilizadas por los ciberdelincuentes para robar información confidencial a los usuarios. De hecho, es relativamente sencillo obtener estos programas maliciosos, ya que existe todo un mercado de venta de troyanos diseñados a la carta y de los denominados kits bancarios, que permiten no solo crear troyanos con múltiples funcionalidades, sino controlarlos y enviarles nuevas instrucciones.

Sin embargo, cada vez más entidades bancarias están tomando medidas de seguridad avanzadas para evitar el robo de información a sus clientes. Es por ello que los ciberdelincuentes también diseñan malware cada vez más sofisticado para intentar saltarse estas medidas de seguridad.

Aún así, no basta con que las entidades bancarias tomen conciencia de esta problemática y adopten medidas para aumentar la seguridad, ya que también los usuarios deben tomar una serie de medidas de precaución para evitar que un troyano bancario se introduzca en sus ordenadores. Para ello, los ciberdelincuentes suelen utilizar técnicas de ingeniería social.

Los usuarios siguen siendo el eslabón más débil de la cadena, y por lo tanto el principal objetivo de los delincuentes

A pesar de que la mayoría de troyanos bancarios que se distribuyen son similares en cuanto a las técnicas que utilizan para robar información, durante este año hemos visto ejemplares que utilizan técnicas realmente sofisticadas, como es el caso del troyano **SilentBanker.D**.

Dicha técnica consiste en que cuando un usuario (que está infectado) realiza una transferencia bancaria, este troyano es capaz de modificar los datos de la persona que va a recibir ese dinero por los datos de la cuenta del ciberdelincuente. Todo esto sin que el usuario se percate de ello, ya que en el comprobante que se le devuelve al usuario una vez realizan la transferencia figura los datos del beneficiario real y no los del ciberdelicuente.

Esto no es algo nuevo, pero este troyano va un paso más allá, de tal forma que se queda residente en el ordenador de la víctima y cuando revisa los movimientos de sus cuentas vuelve a falsificar la información, de tal forma que a no ser que el usuario acuda a su oficina bancaria no se percatará del robo.

Los troyanos bancarios son junto con los rogueware o falsos antivirus las categorías más rentables para los ciberdelincuentes.

2009, el año del Conficker

El Conficker es sin duda el malware más destacado de 2009, no solo por la repercusión mediática que ha tenido y por la cantidad de infecciones que ha ocasionado en ordenadores de todo el mundo, sino porque nos recuerda a las grandes epidemias de antaño.

Expertos en seguridad estiman que el gusano Conficker ya ha infectado más de 7 millones de ordenadores en el mundo

Ya ha pasado más de un año desde la aparición del Conficker y aún se sigue hablando de él. El parche para la vulnerabilidad que explotaba el Conficker (MS08-067) fue publicado por Microsoft en octubre de 2008.

Aún así, más de un año después de la publicación de su parche y de su primera aparición (noviembre 2008) el Conficker sigue activo e infectando ordenadores.

Entonces, ¿cómo es posible que continúe habiendo infecciones?

Todas las empresas actualmente tienen protegido su perímetro (firewall, etc), pero aún así nada impide que un trabajador llegue con su llave de casa, lo conecte a la estación de trabajo y extienda ese código malicioso por toda la red. Además, al afectar a todo tipo de dispositivos USB, afecta a todo tipo de reproductores MP3, móviles, cámaras, etc. Para mitigar este riesgo basta con utilizar herramientas como la **vacuna gratuita de USBs** que hemos lanzado en 2009 y nos permite proteger gratuitamente no sólo a nuestro ordenador, sino a todo tipo de dispositivos USB.

Además de esto, otro motivo de la prevalencia actual del gusano, es que hay mucha gente que utiliza copias piratas de Windows, y por temor a que estas copias sean detectadas no aplican las actualizaciones de seguridad que Microsoft publica periódicamente. Realmente, Microsoft, aunque la copia de su sistema operativo no sea legal, permite realizar las actualizaciones críticas sin ningún tipo de restricción.

La difusión del Conficker fue de tal alcance que se vieron afectadas instituciones de todo tipo. Algunas de las víctimas fueron organismos militares de Gran Bretaña y Francia, universidades como la de Utah en Estados Unidos, etc.

Microsoft llegó incluso a ofrecer una recompensa económica de 250.000$ a quienes proporcionasen información sobre los creadores de este malware.

Las cifras de spam durante este año se han mantenido muy altas: en 2009, el 92% del correo mundial ha sido spam. Como siempre decimos, éste tiene diferentes objetivos, como la venta de productos ilegales, la redirección de tráfico a webs falsas que pueden infectar los equipos, e incluso la distribución directa de malware.

Hemos realizado un estudio en 2009 sobre cómo afectaba el spam por sector industrial. Para ello, hemos analizado en detalle el tráfico generado por el correo electrónico de 867 empresas pertenecientes a 11 sectores diferentes (con base y presencia directa o indirecta con oficinas en 22 países, tanto europeos como americanos). En total, se han analizado más de 2.000 millones de mensajes. El objetivo de dicho estudio era averiguar si las compañías estaban más o menos impactadas por spam y malware dependiendo del sector al que pertenecían, o si este dato era irrelevante.

La principal conclusión de dicho estudio es que el sector **automovilístico** y el **eléctrico**, seguido por el **gubernamental**, copan el top 3 del ranking de mayor recepción de spam y malware a través del correo electrónico, con un 99,89%, un 99,78% y un 99,60%, respectivamente. Esto quiere decir, que de todo el tráfico que se recibe en las empresas, este porcentaje corresponde a e-mails no solicitados o maliciosos. Otra forma de verlo, es que sólo el 0,11% del correo de las empresas del ramo automovilístico es totalmente lícito; el 0,22%, del sector eléctrico, y el 0,40%, del gubernamental.

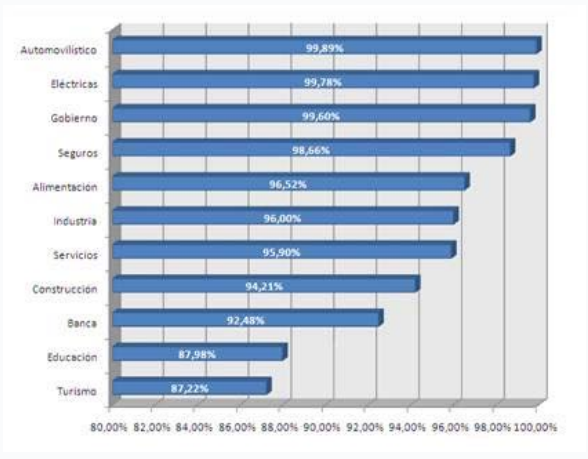


FIG.14

INCIDENCIA DEL SPAM EN EL SECTOR INDUSTRIAL

Curiosamente, el sector de la banca, que a priori sería un candidato óptimo para situarse en el top, se encuentra casi al final de la lista, con un 92,48%. Las cifras más bajas las registra el sector **educativo**, con un 87,98%, y el **turístico**, con un 87,22%.

Tomando en consideración el tipo de spam recibido por sector, no se aprecian prácticamente diferencias en cuanto a sus temáticas. La mayoría, más de un 68%, son relativos a productos farmacéuticos. La segunda categoría, un 18%, la ocupa la venta de complementos falsificados, y le sigue la temática sexual, con un 11%.

Respecto al tipo de malware recibido, el top lo encabezan troyanos bancarios, con un 70% de las detecciones. Le siguen el adware / spyware, con un 22%, y el resto se reparte entre virus, gusanos, etc.

A lo largo del 2009 ha habido numerosos ataques de spam con malware de los que destacamos los siguientes:

- La utilización de noticias actuales e impactantes, sean verídicas o no, sigue teniendo tirón a la hora de distribuir malware en mensajes de spam.

En enero de 2009 se detectaron mensajes de spam para distribuir troyanos bancarios que utilizaban una **noticia de la CNN sobre el conflicto en Gaza**. Estos mensajes contenían un enlace que, una vez pulsado, redirigía al usuario a una página web similar a la de la CNN en la que se podía obtener más información e incluso ver un impactante video. Cuando el usuario se disponía a reproducir el video, aparecía un mensaje informando que es necesario actualizar la versión del Flash Player y le ofrece la opción de descargar una versión más nueva. Es en ese momento cuando se descarga y ejecuta el troyano.

También en enero tuvo lugar un envío masivo de mensajes de spam para distribuir malware, esta vez de trataba de la familia de gusanos Waledac, caracterizada por propagarse en mensajes de correo electrónico utilizando técnicas de ingeniería social. En esta ocasión se hacían eco de la noticia de la renuncia de Barack Obama a continuar en la presidencia de Estados Unidos. Para hacer más creíble la noticia, el usuario era redirigido a lo que parecía la web oficial del presidente, en la que se podía ampliar la noticia.

En febrero le tocó el turno a otro político; en este caso a Tony Blair, ex primer ministro de Reino Unido. La **impactante noticia sobre su muerte** estuvo circulando en mensajes de spam utilizados para distribuir troyanos bancarios. Estos mensajes contenían un enlace a la noticia, que redirigía a una página muy similar a la de la BBC. La noticia venía acompañada de un video que para poder reproducirlo solicitaba la descarga de una versión más reciente de Flash Player.

La noticia de la muerte de Michael Jackson tuvo una gran repercusión no solo por lo inesperado de la noticia en sí, sino por las especulaciones que saltaron en torno a las causas de su muerte. Era de esperar que comenzaran a circular mensajes de spam que aprovecharan esta noticia para distribuir malware. Los rumores sobre la posibilidad de que hubiera sido asesinado dieron lugar a mensajes de spam como el siguiente, que seguramente lograrían despertar la curiosidad de muchos:

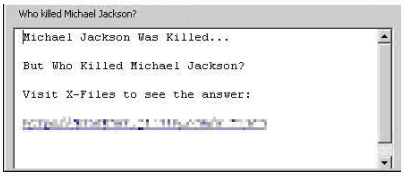


FIG.15

MENSAJE DE SPAM SOBRE LA MUERTE DE MICHAEL JACKSON

- Otro de los trucos y artimañas utilizadas por los ciberdelicuentes para distribuir malware es el envío de mensajes que contienen facturas, comprobantes de productos que el usuario supuestamente ha adquirido a través de Internet, como billetes de avión, y mensajes que parecen ser enviados por empresas de mensajería informando al usuario que no se ha podido realizar la entrega del paquete que envió.

En enero se detectaron varios ataques para distribuir troyanos en mensajes que parecían ser enviados por **diversas compañías aéreas de Estados Unidos**. El adjunto de estos mensajes contenía un billete de avión supuestamente adquirido por el usuario. Ante este hecho, muchos usuarios podrían alarmarse y caer en la trampa por la posibilidad de que su tarjeta de crédito pudiera haber sido utilizada de manera fraudulenta.

A lo largo de todo el año se han detectado mensajes de spam que parecían haber sido enviados por compañías de mensajería, como UPS o DHL, informando a los usuarios que el paquete que envió no ha podido ser entregado por problemas con la dirección del destinatario y le instan a que imprima el comprobante que está adjunto y que pase a recoger el paquete por la oficina, como es el caso del siguiente mensaje:

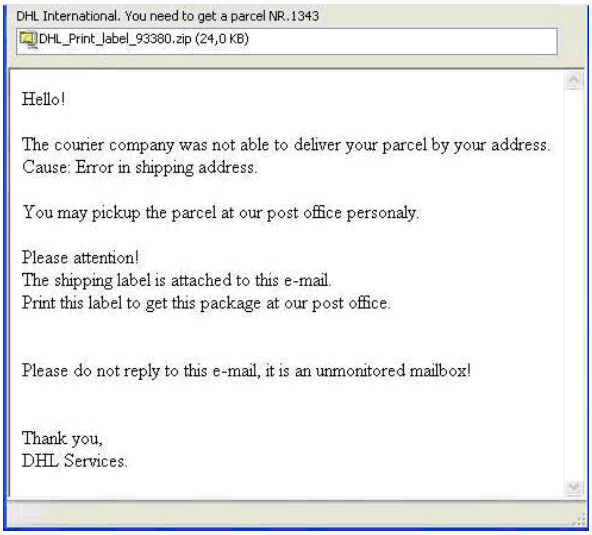


FIG.16

MENSAJE DE SPAM QUE UTILIZA LA EMPRESA DE MENSAJERÍA DHL

- Por último, no debemos olvidarnos de otro de los temas estrella del año 2009: la gripe A. Es un tema serio y que ha generado y sigue generando mucha alarma en todo el mundo, así que no es de extrañar que cualquier noticia relacionada con la gripe A sea tomada en serio por los usuarios y los ciberdelincuentes se aprovechen del temor que despierta ese tema.

En diciembre, comenzaron a circular mensajes de correo electrónico sobre la gripe A para distribuir ejemplares de **troyanos bancarios**. En concreto el mensaje trataba sobre un supuesto programa de vacunación del virus H1N1 para el que se solicita al usuario que cree un perfil de vacunación personal en cierta página web. El mensaje incluye un enlace a dicha página web.

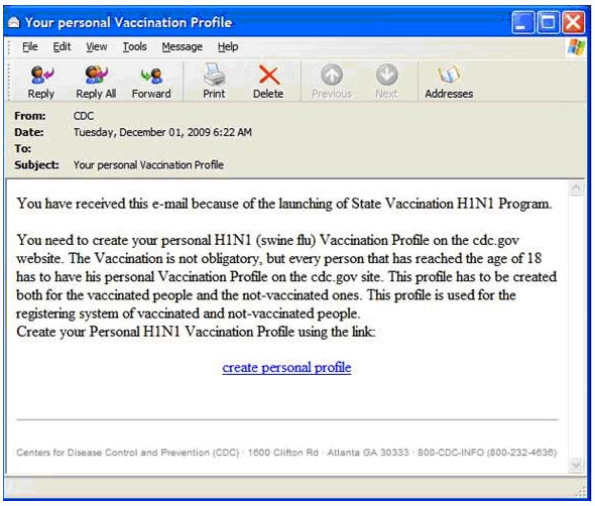


FIG.17

MENSAJE DE SPAM SOBRE LA GRIPE A

Comenzamos el año 2009, a punto de finalizar mientras esta nota se escribe, con varios exploits públicos para vulnerabilidades en productos Oracle. La vulnerabilidad con mayor repercusión dado el número de máquinas afectadas en internet (CVE-2008-5457) afectaba a todos los servidores de aplicaciones J2EE Bea WebLogic. La falla en cuestión podía ser explotada sin necesidad de disponer de un usuario y contraseña de manera remota, una clasificación de 10 sobre 10 en la escala **CVSS2**. De este modo, uno de los servidores de aplicaciones más utilizado en general se veía afectado por un grave fallo que permitía tomar remotamente el control de la máquina o máquinas en las que se hospedaba dicho servidor de aplicaciones.

Habría que esperar hasta mayo para encontrarse con otra vulnerabilidad de gran repercusión, cuando apareció un bug que afectaba a todos los servidores Microsoft Internet Information Server que tuvieran habilitado WebDAV. La misma, CVE-2009-1535, al igual que en el caso anterior, podía ser explotada previa autenticación, si bien en este caso, la vulnerabilidad simplemente permitía obtener acceso a archivos que, de otro modo, sería denegado, esto es, una forma de saltarse la autenticación y la validación de acceso a recursos.

Durante el resto del año aparecieron las ya muy tristemente habituales vulnerabilidades en productos de uso cotidiano tales como navegadores o suites ofimáticas: fallas en Microsoft Internet Explorer, Mozilla Firefox, Google Chrome, Adobe Acrobat Reader (producto del que se hablará en profundidad más adelante), Microsoft Office, OpenOffice, Fox IT Reader, etc. El número de fallos que afectan a dichos productos es realmente alarmante, si bien "esperado", ya que dichas aplicaciones han llegado a un grado de complejidad tan alto que la introducción de nuevos bugs se hace bastante más fácil que en software mucho más simple: A mayor complejidad del software, mayor es también la posibilidad de introducir una falla.

En septiembre aparecerá la que, sin lugar dudas, es la vulnerabilidad más importante del año 2009 (CVE-2009-3103). Laurent Gaffié anunció en Full Disclosure el descubrimiento de un bug incorrectamente clasificado por él como una simple denegación de servicio. De haberse demostrado este extremo, no habría sido sino una molestia pero, lejos de serlo, este fallo que afectaba a todas las versiones de Microsoft Windows a partir de Vista (incluyendo este último) era una extremadamente grave vulnerabilidad de ejecución de código remota previa autenticación en kernel, para más inri.

El investigador Rubén Santamarta, al día siguiente de aparecer la nota de Laurent Gaffié publicó otra nota en la que ofrecía detalles técnicos de la vulnerabilidad. La falla era un clásico "out-of-bounds dereference". En el driver srv2.sys, en la función Smb2ValidateProviderCallback, uno de los campos de la cabecera de paquetes SMB2 (concretamente el campo Process_ID_High) era utilizado como índice en una matriz de funciones pero, y aquí está la vulnerabilidad, sin verificar que el índice pasado estuviera dentro del rango del tamaño de dicha matriz, así pues, accedía a memoria más allá de dicha tabla de funciones e intentaba ejecutar finalmente aquel puntero que hubiera encontrado.

Esta falla tardó bastante en ser explotada de modo fiable, teniendo en cuenta que "bastante" en el terreno de la explotación de vulnerabilidades en software suele ser inferior a un día. Los primeros en publicitar la posesión de exploit remoto fiable que permitiera tomar el control de la máquina afectada fueron los americanos Immunity Sec, concretamente, el encargado de escribir el complejo exploit fue Kostya Kortchinsky. Este exploit fue ofrecido en exclusiva a sus clientes.

A pesar de la gravedad de la última vulnerabilidad comentada, la mención de honor es para Adobe por su dudoso mérito en ser la empresa que durante más tiempo ha dejado a sus clientes siendo vulnerables así como de ser el fabricante de los productos más explotados del año. En total, en el presente año han sido reportadas 45 vulnerabilidades en software de dicha empresa. Comparando con otros paquetes de software, como por ejemplo Microsoft Windows (todo el sistema operativo y aplicaciones base), han sido corregidas 41 vulnerabilidades, así pues, este año se han encontrado más vulnerabilidades en software Adobe (Acrobat Reader y Flash Player) que en todo un sistema operativo. Por si esto fuera poco, lo más preocupante de este triste récord es que la ventana de tiempo en la que los usuarios de sus productos han sido vulnerables ha superado los 30 días en la mayoría de los casos. Pero la guinda del pastel es el 0day que ha aparecido en Adobe Acrobat Reader tan solo 2 días antes de comenzar a escribir este artículo. Un año digno de olvidar para Adobe.

Más nubes en el horizonte de la seguridad

Bienvenidos a la nube. En 2007 sacamos nuestro primer producto que comenzó a utilizar la nube, ahora en 2009 todos nuestros productos la utilizan y hemos lanzado el primer antivirus basado 100% en la nube: CloudAntivirus. Durante este mismo año hemos visto cómo algunos de los grandes fabricantes de soluciones de seguridad han seguido nuestros pasos y han venido a la nube. Este año 2010 será el año donde todas las compañías antimalware que quieran ofrecer protección en tiempo real se subirán a este carro. Las que no lo hagan se quedarán atrás.

Inundación de malware

La cantidad de malware va a seguir aumentando de forma exponencial. La mayor rapidez que otorgan las tecnologías basadas en la nube, como la Inteligencia Colectiva de Panda, llevará a los creadores de malware a ir más allá en la creación de nuevos ejemplares para tratar de evitar su detección y eliminación. La mayoría de las infecciones tendrán como finalidad el beneficio económico, al igual que en los últimos años, por lo que principalmente veremos rogueware, bots y troyanos bancarios.

Ingeniería social

Para infectar, los criminales se focalizarán en técnicas de ingeniería social aplicadas especialmente a buscadores (técnicas BlackHat SEO) y a redes sociales, así como a infecciones desde páginas web, conocidas como drive-by-download.

Windows 7 afectará al desarrollo de malware

Así como Windows Vista no tuvo apenas repercusión, Windows 7 sí la va a tener. Uno de los motivos es la gran aceptación que está teniendo por parte del público, pero de cara al nuevo malware que se cree, el hecho de que la práctica totalidad de equipos nuevos venga con Windows 7 en su sabor de 64 bits es lo que va a forzar a los cibercriminales a adaptar el malware para poder sacar provecho de esta plataforma y asegurar su correcto funcionamiento. Esto va a ser algo que llevará tiempo, pero prevemos que en los 2 próximos años va a suponer un cambio importante.

Móviles

¿Será 2010 el año del malware para móviles? Varias compañías de seguridad llevan tiempo anunciando que el momento en el que el malware para móviles sea tan común como en el PC está llegando. Lamentamos aguarles la fiesta, pero 2010 tampoco va a ser el año de las amenazas para móviles. El PC es una plataforma homogénea, donde el 90% de todos los ordenadores del mundo llevan el sistema operativo Windows sobre hardware Intel, lo que implica que cuando se crea un nuevo troyano, gusano, etc. son posibles víctimas este 90% de ordenadores. El panorama en los móviles es mucho más heterogéneo, con multitud de fabricantes diferentes, que emplean hardware diferente y sistemas operativos diferentes. Incluso dentro del mismo sistema operativo dependiendo de la versión las aplicaciones pueden no ser compatibles.

Por todo esto es muy improbable que 2010 sea el año del malware para móviles. En cualquier caso 2010 va a ser un año con cambios en el mundo de la telefonía móvil, con cada vez más smartphones que dan prácticamente las mismas prestaciones que un PC, la aparición del Google Phone –primer teléfono vendido directamente por Google y además libre, sin ataduras con ninguna operadora-, la cada vez mayor popularidad de Android, y por supuesto el éxito que está siendo el iPhone. Si en unos años quedan sólo las 2 ó 3 plataformas más populares y a esto le sumamos que se popularicen los sistemas de pagos a través de móviles, sí podríamos hablar de un caldo de cultivo que atraería a los ciberdelincuentes.

Mac

Mac, ¿llega el peligro? La cuota de mercado de Mac lleva subiendo los últimos años. Aunque aún no ha alcanzado la masa crítica para que sea tan rentable como los PCs, sí que es cierto que cada vez es más apetitoso para los cibercriminales. El Mac se usa al igual que el PC para acceder a redes sociales, correo, navegación y estos son los principales sistemas de distribución de malware utilizados por los ciberdelincuentes. Esto hace que los Mac ya no sean esa "isla" donde no tienes que preocuparte por los ataques de malware. Los cibercriminales son capaces de distinguir si el sistema a atacar es un Mac, y en ese caso tienen malware preparado específicamente para ellos. En 2009 hemos visto bastantes ataques y en 2010 crecerán.

Nube

Los servicios basados en la nube no sólo son usados desde el punto de vista de la seguridad. Cada vez usamos más servicios basados en la nube sin percatarnos. ¿Quién no utiliza Hotmail o Gmail como correo electrónico, o Flickr para almacenar sus fotos? Pero los servicios basados en

nube no sólo se limitan al almacenamiento, sino también al procesamiento de los datos. Es una herramienta que puede ahorrar mucho dinero en inversiones a empresas, lo que hace que su popularización esté creciendo muy rápidamente. Este hecho hace que los ataques a infraestructuras / servicios basados en la nube sea mucho más probable.

Ciberguerra

Este término, que solemos asociar más a películas de ciencia ficción que a la vida real, lo escucharemos cada vez más. A lo largo de 2009, diferentes gobiernos de todo el mundo, como Estados Unidos, Reino Unido o España, han mostrado la preocupación que tienen ante ataques que puedan afectar a la economía del país o incluso a otras áreas, tales como las denominadas infraestructuras críticas. También este año 2009 vimos un ataque lanzado a diferentes páginas web de Estados Unidos y Corea del Sur, y se sospecha –sin haber podido probarlo aún- que Corea del Norte podría estar detrás del mismo. En 2010 es bastante probable que veamos ataques similares, con motivaciones políticas detrás de los mismos.

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/**