timefor
yourbusiness

WHITE PAPER

Cómo proteger su empresa frente a las amenazas de Internet, liberando tiempo para su negocio.

PANDA SECURITY | 20 Aniversario 1990-2010

www.pandasecurity.com

Cómo proteger su empresa frente a las amenazas de Internet, liberando tiempo para su negocio.

Índice

1. ¿Pueden estar las empresas tranquilas frente al aumento de malware?

Hace ya tiempo que pasó la época de las grandes epidemias, aquéllas en que las portadas de los telediarios y los principales medios de comunicación se hacían eco de infecciones tipo ILoveYou o Sircam. Por aquel entonces los hackers buscaban la fama, ser los pioneros, infectar más número de ordenadores en menos tiempo.

Ahora, en pleno siglo XXI, la situación es otra. Desde hace tiempo los fabricantes de seguridad venimos advirtiendo del nivel de "profesionalización" logrado por los hackers y de cómo están centrando sus esfuerzos en la obtención de beneficios económicos. Para ello emplean tácticas de engaño que repercuten directamente en los usuarios, ya sean éstos empresas o usuarios finales.

Por una parte, las empresas ven cómo sus esfuerzos por mantenerse a salvo de la situación no dan los frutos esperados. Por otro lado, los fabricantes de seguridad nos hemos visto obligados a modificar nuestro modelo de seguridad para afrontar la situación de amenaza que vivimos a diario.

1.1. La gran avalancha de malware

En los últimos años el malware ha aumentado rápidamente, tanto en volumen como en sofisticación. La gráfica inferior muestra la evolución del malware entre los años 2003 y 2006, período de tiempo en el que la cantidad de ejemplares en circulación se duplicaba cada año:

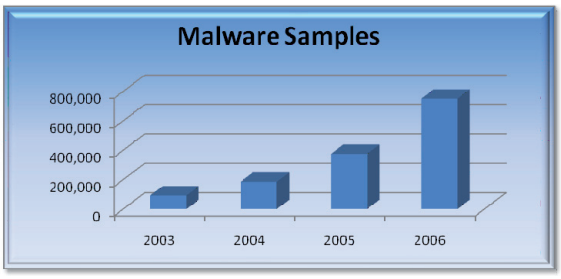

Fig 1. Evolución del malware 2003-2006.

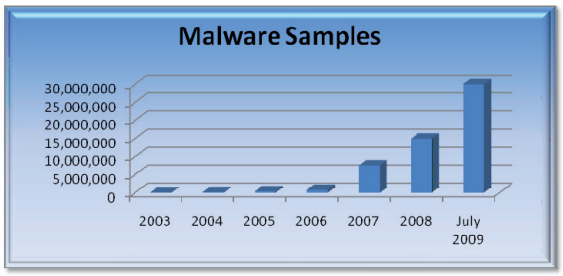

Fig 2. Evolución del malware 2003-Julio 2009.

Hace aproximadamente cinco años, sólo existían 92.000 ejemplares, mientras que a finales del 2008 había unos 15 millones. En julio de 2009, PandaLabs había detectado ya más de 30 millones de ejemplares de malware, y a final de año se superaron los 40 millones.

El motivo de este espectacular aumento está claro: el dinero. El año 2003 fue el del descubrimiento de los troyanos bancarios, códigos maliciosos diseñados para robar las credenciales de acceso a servicios de banca online. En la actualidad, debido a su continua evolución, estos troyanos son una de las formas más habituales de malware.

Pero su capacidad innovadora no se detiene, y cada día surgen variantes más depuradas tecnológicamente y dirigidas a esquivar las medidas de seguridad de los bancos.

Con el fin de intentar contrarrestar los esfuerzos de los cibercriminales varias organizaciones, entre ellas el Anti-Phishing Working Group (www.antiphishing.org), han intentado cohesionar a los diversos miembros de la industria de seguridad informática. Sin embargo, se trata de una batalla larga y dura, y ni siquiera está claro si podremos ganarla alguna vez.

En general, el motivo de que se creen más troyanos bancarios, keyloggers y bots que ningún otro tipo de malware es que resultan ser los más útiles para el robo de identidad. Los datos son irrefutables. En el año 2005, casi la mitad de los nuevos códigos maliciosos eran troyanos:

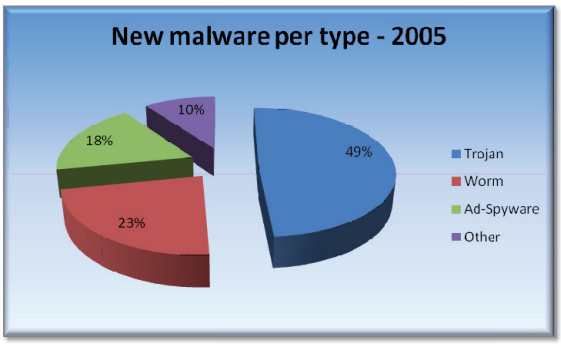

Fig 3. Tipos de nuevo malware 2005.

En la actualidad la situación es mucho peor, ya que los troyanos suponen el 66 % del nuevo malware:

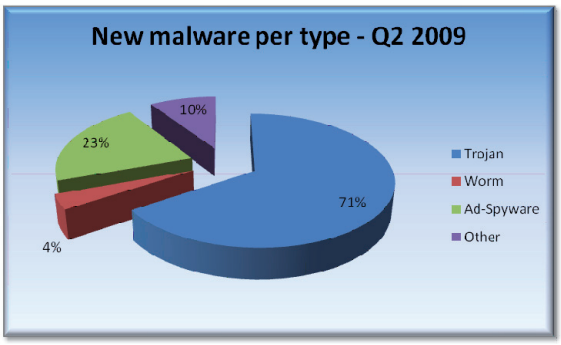

Fig 4. Tipos de nuevo malware 2do. trimestre 2009.

En segunda posición está la categoría de los adware, con un 17,62%, dentro de la que están englobados los conocidos como rogueware o falsos antivirus, a los que por su especificidad dedicamos un apartado más adelante.

Cabe destacar el tercer puesto, con un 6,61%, ocupado por los virus, categoría de malware que parecía estar debilitándose pero que ha resurgido, gracias a versiones nuevas de viejos conocidos como Virutas y Sality.

Y finalmente cierra la clasificación el spyware, con un 5,70%, y los gusanos, que tan solo representan un 3,42%. Pero no hay que bajar la guardia ni menospreciar a estos últimos, ya que a pesar del reducido porcentaje, uno solo de estos gusanos, Conficker, ha traído de cabeza durante todo el año a usuarios y empresas. A fecha de hoy continúa aún infectando ordenadores.

Al igual que en cualquier otro negocio, los cibercriminales persiguen la máxima eficacia. Por eso el creador de un troyano emplea un tiempo fundamental en reflexionar acerca de a qué plataformas afectará su creación y cuántas serán sus víctimas potenciales. Lógicamente, como consecuencia de este análisis, Windows es, por su elevado número de usuarios, la plataforma atacada en más del 99 % de los casos.

Como hemos visto, los troyanos bancarios son la herramienta perfecta para obtener información sobre los usuarios y sus claves, pero esta información no es útil si no ayuda a lograr el objetivo de los cibercriminales: el dinero. Para ello, utilizan métodos cada vez más innovadores.

1.2. Nuevas tendencias de infección

En la medida que los fabricantes de soluciones de seguridad somos capaces de detectar mayor número de nuevas amenazas y de cubrir diferentes frentes de infección, los hackers descubren y explotan otros.

Siempre se ha mencionado las infecciones que se pueden originar a través de la navegación web y cuáles son sus causas: el acceso a sitios web poco recomendables que infectan al usuario sin su conocimiento, la descarga de material procedente de fuentes poco fiables, etc.

Pero últimamente la tendencia en los métodos de infección viene marcada por el acceso a las potenciales víctimas por medio de técnicas llamadas BlackHat SEO.

Los ataques de BlackHat SEO no son algo nuevo, aunque sí que hemos visto un incremento importante en el segundo trimestre del año 2009. SEO son las siglas en inglés de Search Engine Optimization (optimización para motores de búsqueda), y básicamente se refiere a las técnicas que se utilizan para lograr que las páginas web mejoren su posicionamiento en los resultados de los motores de búsqueda (Yahoo, Google, etc.). BlackHat SEO es, por tanto, el uso interesado que los cibercriminales hacen de las técnicas SEO para conseguir que sus páginas aparezcan en estas primeras posiciones.

A modo de ejemplo cabe reseñar lo sucedido el día 1 de junio cuando 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 se obtenía era una página maliciosa. Así, buscando páginas creadas por los mismos cibercriminales nos encontramos con las siguientes páginas relativas a diferentes temas:

16.000 links "TV Online"
16.000 links "YouTube"
10.500 links "France" (Airline Crash)
8.930 links "Microsoft" (Project Natal)
3.380 links "E3"
2.900 links "Eminem" (MTV Awards /Bruno Incident)
2.850 links "Sony"

Por si esto no fuera suficiente, otras tácticas novedosas utilizadas para infectar a los usuarios han tenido a YouTube como escenario. Básicamente, 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 cibercriminales crearon cuentas que insertaban 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, lo que da una idea de la capacidad de infección que pueden llegar a desarrollar.

Como hemos comentado, la imaginación y la innovación de los cibercriminales aumenta y se adapta a las nuevas aplicaciones y plataformas de utilización masiva, como es el caso de las redes sociales (Twitter y Facebook) y comunidades 2.0.

En el caso de Twitter, en abril apareció un gusano que, utilizando una técnica de cross-site scripting, infectaba a los usuarios cuando visitaban los perfiles de usuarios infectados. El gusano infectaba también el perfil del usuario visitante, y continuaba la propagación. Poco tiempo después surgieron nuevas variantes, y finalmente se descubrió que su creador era un joven llamado Mikey Mooney que pretendía atraer usuarios a un servicio competidor de Twitter.

A principios de junio comenzaron a aparecer ataques en Twitter que utilizaban técnicas de infección derivadas del BlackHat SEO, pero convenientemente adaptadas a la especificidad de los usuarios de Twitter. Esta técnica se aprovechaba de una funcionalidad de Twitter denominada "Twitter Trends", que básicamente es un listado de los temas más tratados en Twitter.

Cuando se accede a ellos, se obtiene un listado de todos los tweets que hay publicados sobre ese tema. Estos temas incluidos en Twitter Trends son a menudo los más leídos por los usuarios, por lo que constituyen una vía perfecta por la que introducir la infección. En esta caso lo que los cibercriminales hacen es escribir tweets sobre los temas que aparecen en Twitter Trends, tweets que incluyen links maliciosos a webs desde las que se instala malware en los equipos de quien las visita. Si bien al principio el ataque se centró en sólo uno de los temas, días más tarde los cibercriminales ampliaron su campo de acción e incluyeron links maliciosos en todos los temas de Twitter Trends. Un ejemplo de ello se produjo con motivo del fallecimiento del actor David Carradine. En unas pocas horas ya había cientos de tweets maliciosos en el tema correspondiente. Hoy en día esto sucede con todos los temas más populares de Twitter.

Los virus tradicionales han pasado a la historia. Ahora los cibercriminales buscan dinero como recompensa a su trabajo, al tiempo que inundan con nuevos ejemplares de malware los laboratorios de seguridad.

Los Troyanos y el malware diseñado para el robo de identidad son los enemigos más comunes. En cuanto a los métodos de distribución que utilizan, se observan dos claras tendencias:

Por una parte no dudan en utilizar cebos que introducen en las redes sociales, sirviéndose de estas plataformas de utilización masiva para aumentar la capacidad de infección de sus creaciones; y por otra, se constata la utilización de prácticas de indexación en buscadores, con el fin de engañar a las potenciales víctimas.

1.3. La actualidad, en cifras

Mediante las cifras podemos obtener una visión global de la amenaza que estamos viviendo.

- Se reciben 50.000 ficheros diarios, de los que 37.000 son nuevo malware. El 99,4% se procesan automáticamente por Inteligencia Colectiva con una media de 6 minutos por cada resolución.
- El 52% del nuevo malware procesado por Inteligencia Colectiva sólo vive durante 24 horas, desapareciendo después.
- Durante el primer trimestre de 2009, Inteligencia Colectiva procesó 4.474.350 ficheros.
- Para hacerlo de forma manual, hubieran sido necesarios 1.898 técnicos y 926.347 horas de trabajo.
- La base de datos de Inteligencia Colectiva ocupa más de 18.000 GB o 148 billones de bits.
- Transformando esta cantidad de información en texto, podríamos escribir 727.373 enciclopedias británicas gracias a los 29 billones de palabras que ocuparía la misma extensión que la base de datos de Inteligencia Colectiva.
- Con esta magnitud, podríamos rellenar casi 33 mil millones de páginas de texto, que si pusiéramos una detrás de la otra impresas físicamente, se podría cubrir una distancia de más de 9 millones de kilómetros o ir y volver a la Luna 12 veces.
- Y si tuviéramos que enviar toda esta información mediante una línea estándar de ADSL, tardaríamos 1.045 días.

1.4. Qué riesgos tiene esta situación para las empresas

Por desgracia, lo más habitual es que esta situación no nos parezca lo suficientemente cercana, y que no nos planteemos qué impacto puede tener para nuestro negocio.

Sin embargo, la lista de riesgos es amplia. Los más evidentes nos pueden venir fácilmente a la cabeza, pero hay otros que no podemos calcular de antemano y que pueden repercutir negativamente en nuestra economía, que es, al fin y al cabo, el fin último de cada proyecto empresarial.

¿Cuáles son estos riesgos?

Lógicamente, todos tienen como resultado último una pérdida económica debida a factores como tener que parar nuestros sistemas, que nuestros empleados pierdan tiempo valioso, o que los cibercriminales consigan acceder a nuestros datos para robarnos dinero.

Pero... ¿alguna vez ha calculado qué impacto puede tener para su negocio que sus clientes pierdan la confianza en su empresa?

Imaginemos que sufre un ataque y su base de datos de clientes queda al descubierto, o que su ordenador manda spam o phishing sin saberlo, o que opera online y todo el que compra en su sitio se ve estafado porque un troyano ha robado sus datos bancarios...

Cuanto mayor es su empresa, a mayores riesgos está sometida...

Lo que para una empresa pequeña "sólo" sería un problema, para compañías más grandes puede significar verdaderos quebraderos de cabeza... imaginemos que una compañía dedicada a las patentes ve cómo la información de prototipos desaparece.

La reacción más natural es la de pensar que no nos puede pasar a nosotros. Dado que no existe un gran impacto mediático del problema, porque la situación salta al dominio público sólo cuando hay un problema, tendemos a pensar que no nos va a tocar.

Sólo los casos más espectaculares salen a la luz. ¿Se ha parado a pensar cuántas empresas se infectan diariamente y, lo que es peor, ni siquiera lo saben?

Pero veamos algunos ejemplos recientes, reales y públicos:

Noviembre de 2008: Tres hospitales de Reino Unido, protegidos por McAfee, se infectan con un virus de 2005 y tienen que paralizar su actividad.

Febrero de 2009: El sistema de Justicia de Houston se paraliza porque deben parar la actividad debido a la infección causada por el virus Conficker.

Mayo de 2009: El FBI y los US Marshals cortan todas sus comunicaciones dado que se han visto afectados por un virus.

Mayo de 2009: Tres hospitales españoles y el servicio de urgencias 112, paralizados debido a la infección de un virus.

Cómo proteger su empresa frente a las amenazas de Internet, liberando tiempo para su negocio.

Febrero de 2009: El 75% de los buques de la Marina Francesa se quedan sin comunicaciones debido a la parálisis de sus sistemas afectados por malware...

Febrero de 2009: El Ministerio de Defensa Británico y el Ejército Francés y Alemán, parados durante varios días debido a la infección de sus sistemas informáticos por un virus.

Febrero de 2009: El Ministerio de Defensa británico aborta el aterrizaje de uno de sus aviones aircraft porque sus sistemas informáticos Windows estaban afectados por un "virus global".

Artículos publicados en medios de comunicación online. Referencias en capítulo final.

2. Vías de infección más comunes

Resulta complicado hacerse una idea de la gran cantidad de amenazas informáticas a las que nos enfrentamos cada día. Se clasifican en muchos tipos diferentes, dependiendo qué busca su autor, cómo se distribuyen, cómo llegan, etc.

Explicarlo sería una tarea ardua y complicada. Pero se puede simplificar atendiendo a las tres vías de contagio más frecuentes, que son las que hay que vigilar.

- Ataques o infecciones que nos llegan a través de correo electrónico.
- Infecciones a través de la navegación web.
- Infecciones a través del propio PC del usuario.

2.1. Ataques o infección a través de correo electrónico

El correo electrónico es, sin duda, una herramienta que se ha implantado en todas las compañías y que constituye una forma de comunicación eficiente, rápida y asequible. Sin embargo, es una de las vías de recepción masivas y habituales de spam, phishing y otros tipos de malware como virus, gusanos y troyanos.

Además del tiempo que se pierde haciendo limpieza del propio buzón, que supone un impacto económico para la organización, nos encontramos con peligros como confiar en la educación del usuario para poder detectar y conocer de antemano qué mensaje tiene riesgo de ser una amenaza.

Por lo tanto, la protección tanto a nivel de servidor como del propio cliente de correo electrónico es fundamental para no dejar la responsabilidad de la infección en manos de nuestros empleados.

2.2. Infecciones a través de navegación web

Mucho más comunes últimamente, su principal riesgo es que se "disfrazan" de contenidos inocentes para conseguir que el usuario se descargue –con o sin su conocimiento– ficheros que pueden estar infectados.

Este es el caso de plugins para ver determinados vídeos, ficheros de programas que parecen lícitos, contenidos en pdf que pueden llevar oculto malware, etc.

Además, el riesgo es más evidente dado que, como hemos comentado, los cibercriminales están profesionalizándose a la hora de hacer pasar webs falsas por webs lícitas. Tal es el nivel de verosimilitud alcanzado que, por ejemplo, podemos estar creyendo acceder a nuestro banco cuando en realidad estamos introduciendo nuestros datos de acceso bancarios en una página "clonada" a tal efecto.

2.3. Infecciones a través del propio PC del usuario

Otro de los grandes riesgos a los que nos podemos enfrentar es a la seguridad del propio PC del usuario. Hay muchos factores que influyen en que se cuele un virus en la organización por motivos como:

- No aplicar las normas fundamentales de seguridad corporativa (por ejemplo, no configurar siempre contraseñas adecuadas).
- No aplicar los parches de seguridad que Microsoft Windows publica de forma regular.
- No tener instalada ninguna protección de seguridad, que el producto instalado no sea adecuado y no cubra todas las posibles amenazas, o que, simplemente, esté desactualizado.
- El usuario es remoto y se conecta desde cualquier sitio, sin disponer de unas políticas de seguridad adecuadas y sin realizar las comprobaciones necesarias, etc.

Los tres principales vectores de infección del malware actual son:

- A través del e-mail.
- Mediante la navegación web.
- Por el propio PC individual del usuario.

Cualquiera de los casos anteriores supone un gran riesgo para la integridad corporativa.

A todo esto hay que sumar no sólo el que se puedan descargar ficheros potencialmente peligrosos de Internet, sino el riesgo que supone la utilización de comunidades o redes sociales para esta práctica, dejando en manos de los usuarios el tomar decisiones sobre qué links pinchar, qué sitios visitar o a qué encuentro online suscribirse.

Además, se ha hecho muy popular el intercambiar información mediante dispositivos de almacenamiento masivo, tipo USBs, que están siendo también utilizados para la distribución de malware.

3. El problema de la seguridad en el tráfico web

Las amenazas procedentes de Internet incrementan su impacto y frecuencia entre las empresas de hoy en día. El correo no deseado ocasiona graves problemas para todas las compañías, ya sea en forma de amenazas de seguridad, consumiendo excesivo ancho de banda o reduciendo la productividad de los usuarios, al permitir la llegada de grandes volúmenes de spam.

Las amenazas más peligrosas procedentes de Internet están dirigidas a las empresas. Estas amenazas por lo general, son motivadas política o económicamente.

Un artículo de BBC News ilustraba dramáticamente esta tendencia. Un ordenador desprotegido Windows XP fue conectado a Internet, sin un software corta fuegos o antivirus, con el fin de determinar cuanto tiempo pasaba antes de que fuera golpeado por algún agente devastador de la red. En solo 8 segundos, el ordenador desprotegido fue golpeado por Sasser, uno de los gusanos más rápidos en expandirse por Internet.

3.1. Ingeniería social

Gran parte del malware se instala en los ordenadores de las víctimas utilizando técnicas de ingeniería social.

La ingeniería social consiste en tratar de conseguir información confidencial de los usuarios mediante su manipulación, o convencerlos de que realicen acciones que van en contra de su política de seguridad.

El cibercrimen y la ingeniería social tienen una relación perfecta: una técnica de ingeniería social cuidadosamente elegida se encarga de convencer a los usuarios de que proporcionen sus datos o instalen el programa malicioso, que se encarga de capturar la información y enviarla a los estafadores.

Los mensajes de correo electrónico que utilizan la ingeniería social siguen siendo una de las principales vías de entrada de malware en los ordenadores de los usuarios. Habitualmente, el malware llega en un archivo adjunto en los mensajes, haciéndose pasar por cualquier tipo de documento que parezca inofensivo: imágenes, documentos Word, Excel.

Sin embargo, no todas las familias de malware se distribuyen a través de adjuntos en mensajes de correo electrónico. Tal es el caso de la familia Waledac, que ha destacado por su alta actividad durante el primer semestre del año. Esta familia se caracteriza principalmente por la variedad de temas que utiliza para su distribución y porque se distribuyen en mensajes de correo electrónico que contienen enlaces a páginas web desde las que se descarga el gusano.

Como novedades que incorpora esta familia respecto a lo que habíamos visto antes, podemos destacar que no utilizan archivos adjuntos sino enlaces desde los que se descarga el malware cuando el usuario accede al mismo. Los creadores de este tipo de malware utilizan esta técnica con el fin de dificultar la detección de los mismos por parte de las compañías de antivirus. Antes bastaba con detectar el archivo adjunto para bloquear fácilmente la amenaza, ya que era la misma en todos los casos. Sin embargo, actualmente es necesario monitorizar y hacer un estudio exhaustivo de los enlaces, puesto que van variando el malware que alojan en función de distintos parámetros al acceder, como por ejemplo la hora, el navegador que se utiliza, la procedencia, etc.

Los ciberdelincuentes se han dado cuenta de que intentar propagar una única muestra no es un método muy efectivo y han optado por esta técnica bastante más eficaz.

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.

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.

3.2. La publicidad dirigida: 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.

3.3. Las redes de BOT: BOTNETS

"Bot" es el diminutivo de la palabra "Robot". Los Bots son pequeños programas que se introducen en el ordenador a través de la navegación web, con un correo electrónico o mediante descargas a través de redes P2P. Una vez instalados, los bots aguardan órdenes de su propietario para ponerse en funcionamiento.

Cuando son varios los ordenadores infectados por un bot hablamos de una Botnet, es decir, una red de ordenadores zombis controlados remotamente por el propietario de los bots. Este propietario da instrucciones que pueden incluir: la propia actualización del bot, la descarga de una nueva amenaza, mostrar publicidad al usuario, el envío de spam o lanzar ataques de denegación de servicio, entre otras. Un ejemplo es el "célebre" Conficker.

Algunas redes pueden llegar a tener decenas de miles de ordenadores zombis bajo control remoto. Es habitual que dichas redes tengan un modelo de negocio que permita a su propietario ganar dinero con ellas. Este es el caso del alquiler de botnets para enviar spam, distribuir phishing, etc. El propietario del botnet cobra dinero por ello, y, usando ordenadores que no son suyos, elimina el rastro que pueda dejar su actividad maliciosa.

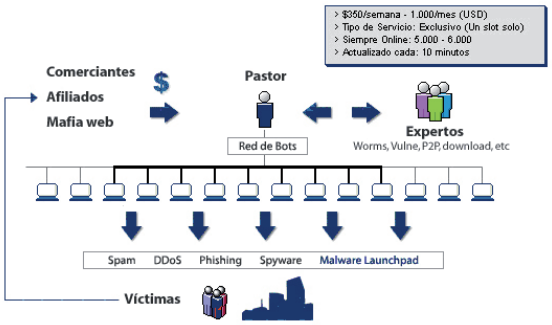

Fig 5. Botnet.

Muchos de estos programas funcionan sobre IRC (Internet Relay Chat), y, de hecho, hay comunidades botnet en las redes IRC donde los hackers se ayudan entre sí o intentan hacerse con la red de zombis de otro hacker.

Panda Security: desarticulación de la botnet Mariposa

Uno de los casos más recientes de redes botnet es el llamado Caso Mariposa. La labor de investigación llevada a cabo por Panda Security, en colaboración con autoridades españolas y el FBI, permitió la desarticulación de una red de ordenadores zombis integrada por más de 13 millones de ordenadores.

De acuerdo con los datos de la investigación, la capacidad de la red era tal que disponía de información personal de más de 800.000 usuarios y podría haber causado daños irreparables si hubiera sido utilizada para casos de ciberterrorismo o ataques masivos como los descritos anteriormente.

Envío de spam, uso más común de las redes de bots

El spam continúa siendo un gran problema incluso hoy en día, hasta el punto de que está considerado en muchos sitios como un delito. Según nuestro laboratorio de investigación PandaLabs, se estima que más del 90% del correo basura procede de redes con ordenadores zombis.

Si el spam viniera de una sola fuente centralizada, sería relativamente fácil seguir el rastro hasta su origen y solicitar al proveedor de servicios de Internet correspondiente que echara abajo la conexión a Internet del origen. El problema estaría solucionado y detener al responsable sería relativamente fácil.

Por eso los ciberdeliencuentes utilizan las redes de bots. El ordenador zombi se convierte en un proxy, y permite al hacker situarse a distancia del origen de los emails de spam. De esta forma, un hacker con una botnet grande, puede enviar millones de mensajes todos los días mientras permanece en una ubicación lejana y segura.

Ataques de denegación de servicio

Algunas veces un hacker utiliza una red de ordenadores zombi para sabotear un sitio Web específico o un servidor de Internet. El proceso es bastante sencillo: un hacker ordena a todos los ordenadores que componen su botnet que contacten con un servidor específico o un sitio Web de forma continuada. Este aumento de tráfico provoca que el sitio Web o el servidor se sobrecarguen, e impide su funcionamiento correcto. En ocasiones este tráfico provocado es suficiente para tirar abajo el sitio de forma definitiva. Estos ataques se denominan ataques de denegación de servicio, también llamados ataques DDoS.

Otra modalidad de ataque DDoS es aquélla en la que se utilizan ordenadores "limpios" como parte de estos ataques. Así es como funciona: el hacker inicia el comando para empezar el ataque desde su ejército de zombis. Cada ordenador dentro del ejército envía una petición de conexión a un ordenador inocente llamado reflector, que interpreta que es el sistema de la víctima quién ha requerido los paquetes de información. Así, cuando los reflectores envían información al sistema de la víctima, éste se resiente ante tantas peticiones de conexión hasta que finalmente se viene abajo al no poder gestionar dichas peticiones y las correspondientes respuestas a la vez.

Desde la perspectiva de la víctima, parece que han sido los reflectores los que han atacado el sistema, mientras que los reflectores interpretan que es el sistema de la víctima quien ha requerido los paquetes de información. Entre bambalinas, los ordenadores zombis se mantienen ocultos y, por supuesto, el hacker preserva su anonimato.

Las víctimas de estos ataques DDoS son innumerables, y entre ellas se encuentran grandes compañías como Microsoft, que sufrió un ataque de este tipo con ejemplares de malware como Blaster o Mydoom. Amazon, eBay, CNN o Yahoo también han sufrido ataques DDoS.

A día de hoy existen determinados ataques DDoS que dadas sus características y modos de actuación se han categorizado y definido, hasta el punto de resultar "familiares". Algunos de ellos son:

- Ping de la muerte - Los bots crean paquetes de datos de gran tamaño y los envían a la víctima.
- Mailbomb - Los bots envían una masiva cantidad de email y echan abajo los servidores de correo.
- Ataque Smurf - Los bots envían mensajes con paquetes ICMP a los reflectores, que a su vez reenvían dichos paquetes a la víctima.
- Teardrop - Los bots envían partes de un paquete ilegítimo y el sistema de la víctima intenta recomponer las partes en un solo paquete. Como resultado el sistema cae.

Fraude en PPC o pago por click

Otra forma de usar los botnet es el *click fraud* o fraude en los clics.

Todos conocemos la modalidad publicitaria que consiste en insertar enlaces publicitarios en una página Web que reportan beneficio económico al propietario de la página, según el número de clics que los visitantes del sitio hacen sobre el enlace en cuestión.

Click fraud es el proceso por el que un hacker configura un botnet para que sus víctimas hagan clic repetidamente en un enlace específico que a menudo está insertado en el propio sitio Web del hacker. De esta forma los hackers obtienen un beneficio económico por los clics fraudulentos.

Una de las cosas que más asusta de estas redes de ordenadores zombis es que podemos acabar siendo víctimas de un robo de identidad o participar en un ataque a una página Web sin ser conscientes de ello. Por eso es importante protegernos contra estas posibles amenazas y saber cómo descubrir si otros ordenadores tienen su seguridad comprometida.

Los datos hablan por sí solos...

Según se desprende de los datos de PandaLabs, cada día se crean cerca de 400.000 nuevos PCs zombis (es decir, ordenadores infectados que esperan órdenes). El período de vida de estos PC zombis es corto, por lo que gran parte de la actividad de los hackers se concentra en la captación de nuevos adeptos para su ejército.

Pero esta cifra va en crecimiento, ya que cada día se crea más malware (en PandaLabs se reciben más de 37.000 nuevos ejemplares diarios), y este malware hay que distribuirlo.

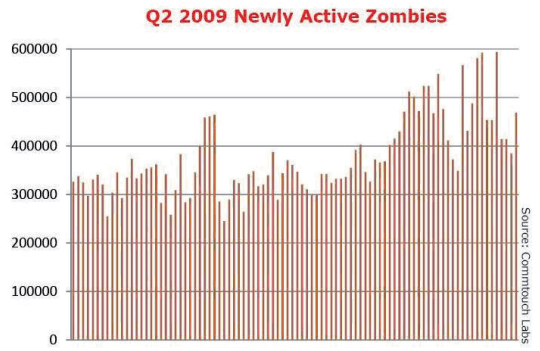

Fig 6. Zombis activos 2do. trimestre 2009.

De acuerdo con el informe trimestral elaborado por Commtouch, el 17,5% del tráfico mundial originado por zombis viene de ordenadores infectados y alojados por el siguiente ranking de ISPs:

1 telesp.net.br
2 veloxzon.com.br
3 ttnet.net.tr
4 tpnet.pl
5 airtelbroadband.in
6 brasiltelecom.net.br
7 asianet.co.th
8 ukrtel.net
9 telecomitalia.it
10 verizon.net

¿Cómo puede perjudicar a su empresa?

Tener ordenadores infectados en una red corporativa puede ocasionar daños cuantiosos, tanto al empresario como a sus clientes y proveedores.

Algunas de las consecuencias son:

- Problemas en la red interna y en las comunicaciones de la compañía.
- Pago excesivo por tráfico de red (en el caso de modelos de pago por consumo).
- Pérdida de productividad de los empleados, por no poder usar correctamente tanto las herramientas ofimáticas como el ordenador en sí mismo.
- Daños a la imagen y reputación corporativas. Por ejemplo, casos como la recepción por parte del cliente de un email en el que se adjunte spam de compra de Viagra, o la existencia de un troyano que sea detectado por la solución de seguridad instalada en el ordenador del cliente o proveedor.
- Riesgo de multas que pueden ir desde simples sanciones administrativas hasta penas de cárcel, dependiendo de para qué se haya usado la red de bots de la que, sin saberlo, formamos parte.
- Percepción de imagen negativa, que puede verse agravada si el problema salta a los medios de comunicación.
- Etc.

Y todo ello, que es lo peor, sin haber sido conscientes, en ningún momento, de estar cometiendo un delito.

Lo mejor es prevenir...

Prevención contra las botnet

¿Qué hacer para que su red no se convierta en una botnet? ¿cómo prevenirlo? Sin ninguna duda teniendo muy claro en todo momento que la prevención es un proceso continuado, que requiere de la puesta en práctica de medidas a tener en cuenta:

- Tener un buen software antimalware instalado y actualizado, protegiendo todos los puntos de la red.
- Si el antimalware no incluye firewall, es recomendable instalar uno, tanto en los puestos como en los servidores.
- Tener una adecuada política de establecimiento y mantenimiento de contraseñas (no pongas el nombre de la empresa, por ejemplo).
- De vez en cuando, realizar auditorías de seguridad en profundidad.
- Proteger también el perímetro de la red, para tener la seguridad de que los equipos de los empleados no se infectan al navegar por Internet.
- Aplicar todos los parches de seguridad que publican los diferentes fabricantes del software utilizado en la empresa (Microsoft, Adobe, etc.).
- Estar al día de las noticias sobre nuevas vías de infección y nuevos métodos utilizados por los cibercriminales.

3.4 Vulnerabilidades

Como en el mito griego de Aquiles, una vulnerabilidad es un punto a través del cual es posible vencer la seguridad de un ordenador. Una vulnerabilidad es un fallo en la programación de una aplicación cualquiera, y puede ser aprovechado para llevar a cabo una intrusión en el ordenador que tenga instalado dicho programa.

Generalmente, dicho fallo de programación se refiere a operaciones que provocan un funcionamiento anormal de la aplicación. Esta situación anómala puede ser producida artificialmente por una persona maliciosa para introducirse en un ordenador sin el consentimiento del usuario. En ocasiones, es suficiente con abrir un documento creado "artesanalmente" con ese fin específico.

Esto le permitirá al usuario malicioso realizar un gran abanico de acciones en el ordenador vulnerable, desde ejecutar ficheros hasta borrarlos, introducir virus, acceder a información, etc.

Aunque son más conocidas las vulnerabilidades asociadas a sistemas operativos, navegadores de Internet y programas de correo electrónico, cualquier programa puede presentar vulnerabilidades.

Por ello, es altamente recomendable estar informado acerca de las vulnerabilidades descubiertas en los programas instalados y aplicar los parches de seguridad más recientes proporcionados por la empresa fabricante, accesibles a través del sitio web de la misma.

4. ¿Y qué dicen las empresas?

Los datos del Barómetro Internacional sobre Seguridad publicado por Panda Security (disponible en www.pandasecurity.com) muestran que la realidad de los empresarios, aparte de lo que conocemos desde los laboratorios de seguridad, es que el malware sí supone un problema y una preocupación en su quehacer diario.

Algunos de los datos más relevantes son los siguientes:

- Un 58% de las empresas ha sufrido alguna vez una infección con malware.
- El 30% de los negocios en Europa ha tenido que detener en alguna ocasión su negocio por esta causa. Además, y también debido a ello, un 36% de las pequeñas y medianas empresas experimentó una pérdida de productividad y un 15% perdió datos importantes.
- Estas infecciones se produjeron a pesar de que el 93% de las PYMEs europeas cuentan con algún sistema de seguridad.
- En lo referente al tipo de protección instalada, el 27% de los negocios que cuentan con un sistema de seguridad tienen instalado software gratuito.
- Al preguntar a las empresas que no disponían de un sistema de seguridad instalado las razones que les habían llevado a ello, en un tercio de los casos señalaron que los sistemas de protección eran muy caros. Además, un 8% declaró que no consideraba necesario contar con protección alguna.
- En cuanto a la importancia del papel que las empresas otorgan a la seguridad, las cifras coinciden, y así, en Europa el 55% de las empresas considera la seguridad muy importante para su actividad. Sin embargo, sólo un 64% de las empresas cuentan con una persona dedicada en exclusiva a la seguridad.

Si las empresas se protegen y son conscientes del problema... ¿qué está causando estos agujeros de seguridad?

Mientras las soluciones tradicionales de seguridad son críticas para una primera línea de defensa, las organizaciones de cualquier tamaño se enfrentan todavía a un importante número de agujeros de seguridad que son continuamente explotados por las técnicas de malware modernas. Hoy en día el malware se infiltra sigilosamente en las redes corporativas por varias razones:

- No existe una estrategia de seguridad que cubra todos los principales vectores de infección.
- Las empresas con oficinas remotas o con usuarios móviles permiten que éstos se conecten a la red con dispositivos que pueden estar infectados.
- No se gestionan de forma correcta oficinas remotas o dispositivos de navegación, por ejemplo.
- Existe poca labor de educación y concienciación acerca de las más modernas técnicas de infección y los últimos trucos, lo que provoca que el uso de tecnologías fáciles de explotar, como P2P, compartición de archivos, tecnologías multimedia y mensajería instantánea, se conviertan en auténticos peligros para la integridad de la red.
- Demasiados ordenadores sin mantenimiento adecuado, o portátiles contratados o invitados, o intercambio de ficheros a través de USB, etc.

5. ¿Cómo estar realmente tranquilos frente al malware y los hackers?

Ante esta situación, la mejor forma de sentirse realmente tranquilo es aliarse con el mejor proveedor de seguridad, que ha de estar capacitado para ofrecerle:

- Tecnología puntera y vanguardista capaz de afrontar el problema.
- Soluciones específicamente diseñadas para conseguir la máxima seguridad para su negocio.
- Un soporte técnico adecuado, efectuado por profesionales que se encarguen de la seguridad de su empresa, y que a usted le permita realmente concentrarse en su actividad.

6. Nuestra visión tecnológica

Panda Security siempre se ha situado a la vanguardia tecnológica del mercado internacional por ofrecer diferentes avances en materia de seguridad antimalware. Como compañía visionaria, Panda Security ha ofrecido al mercado sus innovaciones con dos años o más de antelación con respecto a otras compañías del segmento de la seguridad informática.

Este es el caso de las tecnologías de detección proactiva TruPrevent, capaces de detectar malware incluso sin conocerlo con anterioridad, que Panda Security lanzó al mercado en el año 2005 y que recientemente han incorporado a sus productos sus competidores.

Si echamos un vistazo a los 20 años de historia de la compañía, esto, que parece sólo un ejemplo, se transforma en la constante que es: la reinversión del 30% de la facturación en I+D+i para conseguir ofrecer siempre la tecnología más puntera de protección.

La actual visión tecnológica de protección de Panda Security tiene como pilar principal el sistema de análisis, clasificación y desinfección automática de malware denominado Inteligencia Colectiva. Además, se basa en ofrecer soluciones bajo arquitectura Nano, cuyo impacto en los recursos globales es mínimo, y englobadas en el modelo de seguridad gestionada como SaaS (Software-as-a-Service).

6.1. Inteligencia Colectiva

El gran aumento de malware que se experimentó de forma notoria en el año 2006 sorprendió a la industria de la seguridad. Fruto de esta situación, detectada por Panda Security, surgió la necesidad de obtener una nueva metodología en los procesos de detección y neutralización de malware, que habrían de ser diferentes a todo lo aplicado hasta entonces y que deberían seguir ofreciendo la máxima protección a nuestros clientes.

El funcionamiento normal de un laboratorio antivirus es que primero tiene que recibir la muestra de malware (el nuevo virus, gusano o troyano), analizarlo por un técnico y crear la vacuna correspondiente que, una vez publicada a través de Internet, sirva para que los usuarios se la descarguen a su fichero de firmas local y estén protegidos por si el nuevo virus les llega.

Este modelo, que tradicionalmente había funcionado, resulta inútil cuando un laboratorio pasa de recibir 100 muestras al día a recibir 37.000 nuevos virus, que es la situación actual.

En este caso, se necesitaría un gran ejército de técnicos de laboratorio que, contra el reloj, fueran capaces de procesar todos los nuevos ejemplares que reciben.

En Panda Security, conscientes de dicha situación, comenzamos a desarrollar en el año 2006 un conjunto de tecnologías basadas en Inteligencia Artificial, a las que denominamos Inteligencia Colectiva, y que son capaces por sí solas de analizar, clasificar y desinfectar el 99,5% de los nuevos ejemplares que cada día recibimos en PandaLabs, manteniendo a nuestros clientes protegidos prácticamente en tiempo real.

Al mismo tiempo, los técnicos de laboratorio se entregan a la tarea de procesar el 0,5% del malware restante, de mayor complejidad técnica o tecnológica y que la Inteligencia Colectiva no es capaz de determinar como malware.

Estas tecnologías se pusieron a disposición del mercado en el año 2007 y en la actualidad todas las soluciones de la compañía se benefician de esta gran base de conocimiento, ofreciendo unos ratios de protección por encima de la media del mercado.

6.2. Arquitectura Nano

Bajo la denominación de arquitectura Nano agrupamos nuestra filosofía de ofrecer la máxima protección a través de soluciones diseñadas para impactar al mínimo el rendimiento del PC.

Intimamente ligadas al concepto de Inteligencia Colectiva, estas soluciones buscan trasladar la máxima operatividad de las aplicaciones de seguridad a lo que se denomina "la nube", o protección desde Internet, de forma que las acciones que se desarrollen o tengan como escenario la infraestructura de nuestros clientes sean sólo las más básicas.

Para explicarlo mejor, hay que seguir el modelo tradicional de funcionamiento sobre el que incidimos: para que una solución de seguridad sea capaz de parar una amenaza, necesita conocerla con anterioridad. Esto implica no sólo la labor del laboratorio, sino que ese conocimiento tiene que estar de alguna manera en la solución instalada.

Las soluciones tradicionales de seguridad funcionan con ficheros de firmas locales y un conjunto de tecnologías de detección proactiva. Esto quiere decir que toda la base de datos del malware conocido tiene que estar en el servidor o en la máquina local. Si contamos con una base de datos de 30 millones de registros de malware únicos y diferentes, todo ese conocimiento tiene que estar en el PC.

El problema que esto conlleva es que cada vez que se recibe un correo electrónico, por ejemplo, el antivirus chequea la información con toda la base de datos, lo que necesariamente consume recursos de la máquina y ralentiza el funcionamiento normal del ordenador.

Con soluciones basadas en arquitectura Nano se arregla el problema trasladando a la "nube" dichas consultas, no necesitando tener toda la base de datos de malware instalada en el PC, y liberando de recursos, de esta manera, el ordenador local.

Esto se traduce en mayor velocidad y mayor disponibilidad de recursos de memoria al ejecutarse determinados procesos en otro sitio, en la nube, y no en la CPU del ordenador.

Muchas de las soluciones del portfolio de Panda Security ya funcionan de esta manera, y todo el resto de soluciones más tradicionales se están adaptando al nuevo modelo de arquitectura.

6.3. Modelo SaaS

Por último, el ofrecer las soluciones de seguridad en modelo SaaS (Software-as-a-Service o Security-as-a-Service) es otra ventaja competitiva. Dichas soluciones, alojadas en Internet y que prestan su servicio desde la "nube", añaden a todas las ventajas mencionadas anteriormente el hecho de que suponen un ahorro muy importante en gastos de infraestructura y, además, facilitan enormemente la gestión de la seguridad, que puede ser incluso facilitada por un tercero (partner, distribuidor, consultoría, etc.).

7. Global Business Protection: Soluciones de seguridad para el tráfico web

Da igual cómo sea el tamaño de su negocio: el malware actual está diseñado para conseguir beneficio económico, y los hackers atacan tanto a las empresas pequeñas como a las grandes.

Desde esta perspectiva, las soluciones Global Business Protection de Panda Security ofrecen un servicio personalizado de seguridad integral para el tráfico web enfocado a sus necesidades y modelo de negocio.

7.1. Protección Hosted

Panda Cloud Internet Protection es una solución de seguridad basada en la nube que garantiza el **acceso seguro y controlado a Internet**. Sin necesidad de gestionar hardware, software ni recursos de la organización.

Panda Cloud Internet Protection garantiza la protección contra amenazas 2.0, permite asignar políticas por cada tipo de usuario y facilita informes completos y en tiempo real.

7.2. Protección On Premise

Panda GateDefender es una familia de appliances que ofrece **protección perimetral** y se ajusta perfectamente a las necesidades de la red.

Esta robusta solución garantiza un control total sobre las políticas web y suministra informes detallados sobre el tráfico.

La combinación de tecnología sólida y protección integral que Panda Global Business Protection ofrece, junto al servicio de soporte continuo 24x7, le proporcionan la tranquilidad necesaria para que usted pueda dedicarse a la actividad principal de su negocio, sin que por ello quede desatendida la seguridad de su empresa.

8. Nuestros clientes dicen de nosotros...

Nuestras soluciones de seguridad están especialmente diseñadas para su tranquilidad, para que centre sus esfuerzos en lo que realmente es importante para usted, y pueda dejar la seguridad de su empresa en manos de verdaderos expertos.

PANDA **CLOUD**OFFICE**PROTECTION**

EADS

"Después de una serie de pruebas con varias soluciones de seguridad (Norton, Avast, Kaspersky y Panda Security), se comprobó que Panda fue el producto que mejor respondía a nuestras expectativas, gracias a su bajo consumo de recursos, su gestión centralizada y la facilidad de despliegue".

Jean-Yves Andreoletti. Gerente de Sistemas y plataformas de integración de redes / Verificación de PMR. EADS Defence & Security. Francia.

AMPER

"Desde el año 1995, en el que decidimos la implantación de Panda en el Grupo Amper, hemos ido constatando año tras año lo acertado de esta decisión".

Manuel Fernández. Director de Informática. Grupo Amper.

ESCUELAS PÍAS

"Una de las mayores ventajas que vemos en Panda Managed Office Protection es el ahorro de costes, mientras tenemos la seguridad de estar protegido contra todo tipo de amenazas, lo que nos proporciona una total tranquilidad".

José María Domínguez. Equipo de Informática de La Provincia Emaús. Escuelas Pías Provincia Emaús. España.

PANDA **CLOUD**INTERNET**PROTECTION** **¡NUEVO!**

SIN CHEW DAILY

"Panda GateDefender es capaz de bloquear amenazas en el perímetro y detectar malware en el tráfico entrante y saliente".

Mr. Ong. Director de la Red Corporativa. Sin Chew Daily. Malasia.

MATCHFRAME VIDEO

"Gracias al filtrado web de GateDefender, hemos sido capaces de incrementar la productividad de nuestros empleados".

Mike Van Fleet. Administrador IT. Matchframe Video. US.

PANDA **CLOUD**EMAIL**PROTECTION**

ORDISMATIC

"Panda Managed Email Protection ha solucionado a nuestros clientes un problema crítico de gestión del spam, liberándoles de las tareas mecánicas de filtrado de correos y su posterior eliminación. A los 7 días de uso valoran el producto del 1 al 10 con un 10".

Joan Vila. Gerente. Ordismatic (partner de Canal). España.

9. Referencias

http://pandalabs.pandasecurity.com

http://www.fayerwayer.com/2008/11/impresentable-hospitales-de-londres-se-contagian-con-virus-informatico/

http://www.theregister.co.uk/2009/02/02/nhs_worm_infection_aftermath/

http://www.theregister.co.uk/2009/03/09/scot_hostpitals_malware_infection/

http://www.theregister.co.uk/2009/02/09/houston_malware_infection/

http://www.madboxpc.com/conficker-el-virus-que-tiene-revolucionado-a-redmond/

http://www.idg.es/pcworld/Conficker-ha-creado-la-mayor-red-bot-del-mundo/doc79409-Seguridad.htm

http://www.eweek.com/c/a/Security/Conficker-Attacks-700-University-of-Utah-PCs-835179/?kc=rss

http://ecodiario.eleconomista.es/noticias/noticias/878925/11/08/Algunos-ordenadores-del-Pentagono-estan-infectadas-por-un-virus.html

http://www.kriptopolis.org/cazas-franceses-en-tierra-por-virus-conficker

http://www.telegraph.co.uk/news/worldnews/europe/france/4547649/French-fighter-planes-grounded-by-computer-virus.html

http://www.kriptopolis.org/virus-colapsa-armada-britanica

http://www.itwire.com/index.php?option=com_content&task=view&id=22716&Itemid=53

http://www.elpais.com/articulo/madrid/virus/cuela/ordenadores/Sanidad/elpepiespmad/20090512elpmad_1/Tes

http://www.theregister.co.uk/2009/05/22/fbi_mystery_viral_infection/

http://www.elmundo.es/elmundo/2009/05/22/navegante/1242982288.html

http://www.cronica.com.mx/nota.php?idc=154655

http://www.elconfidencialdigital.com/Articulo.aspx?IdObjeto=16025

http://terranoticias.terra.es/nacional/articulo/ejercito-virus-ataco-centenares-ordenadores-3074699.htm

http://www.pandasecurity.com/spain/homeusers/media/press-releases/viewnews?noticia=9702

http://www.pandasecurity.com/spain/homeusers/security-info/tools/reports/

http://www.pandasecurity.com/spain/homeusers/media/press-releases/viewnews?noticia=10084

PANDA SECURITY

Delegación Bilbao
Gran Vía Don Diego López de Haro, 4
48001. Bilbao. ESPAÑA
Tlf: 94 425 11 00 - Fax: 94 434 35 65

Delegación Madrid
Ronda de Poniente, 17
28760. Tres Cantos. Madrid. ESPAÑA
Tlf: 91 806 37 00 - Fax: 91 804 35 29

Delegación Barcelona
Avda. Diagonal, 420 - 2º, 1
08037. Barcelona. ESPAÑA
Tlf: 93 208 73 00 - Fax: 93 458 59 00

Delegación Valencia
Doctor Zamenhof, 20 Bajo
46008. Valencia. ESPAÑA
Tlf: 96 382 49 53 - Fax: 96 385 93 80

902 24 36 54
www.pandasecurity.com

PANDA SECURITY | 20 Aniversario 1990-2010