

# Networkers

Webmasters

« Selección de plugins WordPress | Inicio

16 Ago 2012

## Redirección 301 : la solución mágica

Escrito por: [José María Amenós Vidal](#) el 16 Ago 2012 - [URL Permanente](#)

Estos días pasados hemos trasladado de DNS y registrador nuestro dominio infocath.com con el fin de conseguir SEO, sin embargo, el problema fundamental era conservar los contenidos y el tráfico para que no se perdieran después de hacer los cambios y ante esta tesitura vimos que la solución a nuestros problemas era migrar nuestra web a estrategia.info y utilizar la redirección 301 incluyendo dos sentencias en nuestro fichero .htaccess en la carpeta pública de archivos FTP de infocath.com.

Por tanto, os proponemos a continuación la solución que hemos encontrado gracias a InternetLab.

RewriteEngine On

```
rewriteCond %{HTTP_HOST}^infocath.com [NC]
rewriteRule ^(.*)$ http://estrategia.info/cath/$1 [R=301,L]
```



RewriteEngine On

```
rewriteCond %{HTTP_HOST}^www.infocath.com [NC]
rewriteRule ^(.*)$ http://estrategia.info/cath/$1 [R=301,L]
```

Con estas rutinas cualquier enlace que empieza por infocath.com (con o sin www) se redirige automáticamente a la carpeta que queramos de la dirección electrónica de estrategia.info consiguiendo así no perder visitantes y apuntar a los mismos contenidos aunque en otro dominio. No obstante, la condición es que se respeten en su integridad las estructuras de los enlaces, para que con la redirección 301 solamente cambie el dominio de origen por el de la carpeta de destino.

Compartir

Me gusta Registrarse para ver qué les gusta a tus amigos.

Twitter 0

0 comentarios Tags: dns validation, networkers community, internetlab, webmaster, seo, htaccess

10 Ago 2012

## Selección de plugins WordPress

Escrito por: [José María Amenós Vidal](#) el 10 Ago 2012 - [URL Permanente](#)

Con el fin de modernizar nuestro sitio en internet estrategia.info hemos cargado en nuestro servidor la última versión de Wordpress 3.4.1 de la que os ofrecemos por orden alfabético y en un extracto los plugins que hemos utilizado para habilitar nuestro sitio en la red.



**Akismet** : anti-spam.

**All in one seo pack** : un plugin básico para optimizar la web de cara a los buscadores que se complementa con Platinum SEO.

**AntiVirus** : solución de seguridad que escanea nuestros archivos buscando código malicioso.

**BackUpWordPress** : se aconseja para realizar una copia de seguridad del sistema de archivos (carpetas FTP y base de datos MySQL).

**Better WP Security** : un completo conjunto de métodos y técnicas que asegurarán el servidor y dominio contra ataques en la red.

**Block Bad Queries** : bloquea los ataques de malware.

**BNS Add Widget** : Panel para información adicional al final de la página.

**Broken Link Checker** : comprobación de enlaces truncados con alertas que nos avisan de los links obsoletos.

**Cbnet Ping Optimizer** : tiene como funcionalidad optimizar pings para que no sean considerados spam.

**Code Markup** : permite introducir entre las etiquetas <code> y </code> diferentes fuentes html, script o php, etc ...

**Contact Form 7** : Formulario de contacto.

**Current Date & Time Widget** : fecha de calendario y reloj horario.

**Custom Query String** : limita el número de entradas a mostrar.

**Dofollow** : deshabilita la propiedad "nofollow" por defecto de wordpress permitiendo la indexación de comentarios en buscadores.

**Dublin Core** : metainformación.

**Global Translator** : Traductor de idiomas.

**Google News Sitemap** : crea un "sitemap" para facilitar el trabajo de los motores de rastreo de Google noticias.

**Google Sitemaps – Append UTW Tags** : añade al mapa del sitio enlaces de etiquetas facilitando la tarea de los robots que rastrean nuestro contenido para indexarlo en los motores de búsqueda.

**Google XML Sitemaps** : un completo "sitemap" de la web para su indexación a través de las herramientas para webmasters de Google.

**Gtmetrix** : nos da ciertas indicaciones de como se está desarrollando en cuanto a rendimiento y velocidad los distintos espacios de nuestra web.

**Jadedcoder Sticky Permalinks** : escaneo automático de las urls del dominio y de los cambios que experimentan cuando se migran contenidos que se encarga de procesar las peticiones de direcciones antiguas hacia las nuevas con el fin de evitar enlaces rotos o notificaciones de error 404.

**Login LockDown** : método de encriptación de la clave de acceso para evitar que sea descifrada.

**Moderate pingbacks & trackbacks** : los pings y trackbacks quedan en cola de espera para su moderación impidiendo que sean publicados sin intervención del administrador.

**NextGEN Gallery & View** : Galería audio-visual, lista de imágenes y pase de diapositivas.

**nRelate Related Content** : sistema utilizado para ofrecer en el oficio de encabezamiento o talonamiento de los posts o páginas estáticas un número determinado de entradas que se publicaron con anterioridad en relación con el tema.

**Paginator** : ofrece un modo de navegación avanzado para nuestro sitio.

**Platinum SEO Pack** : completa las funciones de All in one seo pack.

**PostPost** : establece diferentes localizaciones a pie o cabecera de página en las que se pueden introducir imágenes, textos u otros recursos digitales.

**Print Friendly and PDF** : funcionalidad para la impresión de documentos en papel o archivos pdf que incluye la posibilidad de su envío por email.

**Quick Page/Post Redirect DEV** : consigue redirigir el tráfico entre distintas direcciones electrónicas internas o externas.

**Related Posts Thumbnails** : Muestra "microkids" y mensajes miniatura de otros posts relativos al contenido tratado en una página o entrada.

**Search Everything** : excluye las páginas que indiquemos de la lista de resultados de nuestro buscador en la web.

**Secure WordPress** : complementa WP Security Scan de Website Defender & Acunetix.

**SEO Friendly Images** : generación automática de etiquetas para imágenes.

**SEO Smart Links** : genera interlinks o enlaces internos de forma automática a partir de categorías y etiquetas.

**SEO Ultimate** : Search Engine Optimization de última generación.

**Share Buttons by Lockers / AddToAny** : modalidad de botones para compartir artículos en diferentes redes sociales.

**Sliding Panel** : Añade un panel superior desplegable cuando nos falta espacio de publicación con los widgets laterales o a pie de página de que disponemos.

**Stream Video Player** : Inserción de videos compatibles en diferentes formatos.

**Subscribe Remind** : inserta un recordatorio a modo de reseña que invita a nuestros usuarios a suscribirse al agregador de noticias.

**The Authenticity Checker (TAC)** : autentifica el código interno de los temas instalados en nuestro wordpress.

**Ultimate Security Checker** : Examina el nivel de prevención y protección en una escala de 0 a 115, teniendo que obtener un mínimo de 90 para una seguridad moderada. Lleva adjunto un tutorial para implementar medidas de mejora en cuanto a seguridad, así como también ofrece la posibilidad de un monitoro web.

**Vitamin** : completa solución SEO, de seguridad, rendimiento y velocidad para nuestro sitio web.

**WordPress Firewall** : cortafuegos.

**WordPress Gzip Compression** : Al utilizar la compresión gzip en el sitio mejora su rendimiento.

**WordPress Importer** : ayuda a la migración de contenidos entre webs.

**WordPress PopUp y Scrolling down popup**: carteles para anuncios flotantes.

**WP Auto Tagger** : generación automática de etiquetas.

**WP CleanFix** : entre sus prestaciones destaca la optimización de la base de datos, la eliminación de los comentarios considerados "spam" y la limpieza en general.

**WP Limit Posts Automatically** : acota el número de palabras, párrafos, etc ... que se deben mostrar en los resúmenes que aparecen en la página principal, al realizar una búsqueda u otros extractos.

**WP Maintenance Mode** : pone en modo mantenimiento a nuestro sitio.

**WP Security Scan** : revisa las vulnerabilidades e indica las soluciones (por ej. cambiar el prefijo wp\_ de los archivos de nuestra base de datos, el nombre de usuario admin que viene por defecto, siendo nuestro consejo hacer ambas maniobras justo en el momento de instalar la versión 3.4.1, y que el plugin comprobará), realiza backups o copias de respaldo de la base de datos entre sus funciones más importantes.

**WpSEO** : completa solución SEO para nuestra web.

**WPTouch** : versión para móvil, ipad u otras plataformas.

**XSPF player** : Gestor y dispositivo para la audición de podcasts.

**Yet Another Related Posts Plugin** : Muestra una lista de las publicaciones anteriores que están relacionadas con cada post y que se incluyen a pie de entrada o en su defecto en el feed de noticias.

Compartir

Me gusta Sign Up para ver qué les gusta a tus amigos.

Twitter 0

0 comentarios Tags: word press, plugin

20 Jul 2012

## Comprobación en materia de seguridad de nuestra web online

Escrito por: [Carmen Martínez Ibáñez](#) el 20 Jul 2012 - [URL Permanente](#)

De las múltiples opciones que hay en el mercado y dentro del amplio abanico de licencias freeware nos centraremos en esta ocasión en un sistema de análisis y evaluación que no es de pago pero que por sus prestaciones ofrece un buen servicio para el usuario. Nos referimos a las diferentes modalidades de examen en línea que proporciona NoVirusThanks & Co.

1. **URLVoid**. Un servicio que permite escanear un dominio a partir de la reputación y listas negras de que disponen los sistemas de motores de búsqueda y bases de datos de compañías de seguridad con garantizada solvencia que permiten detectar un sitio peligroso en la red. [Ver demo](#).

2. **Multi-Engine Antivirus Scan File & Web Adress**. Si usted tiene un archivo sospechoso o una web vulnerable que pueda presentar posibles problemas de seguridad por este medio analizará el fichero o la página electrónica utilizando para ello múltiples antivirus que le informarán del resultado de su análisis. Al enviar archivos o direcciones electrónicas en el siguiente formulario usted está de acuerdo con los Términos de Servicio y la Política de privacidad. [Ver demo](#).

3. **ScanURLs**. Analiza las URLs en tiempo real a partir de una completa base de datos de firmas de malware para detectar la presencia de código malicioso. Los motores de análisis se actualizan frecuentemente para asegurar la detección de las últimas y más nuevas inyecciones en la red de software malintencionado. El uso es simple, escribir la URL que se desea analizar y pulsar el botón de escaneo. Después de unos segundos, verá el informe de seguridad del sitio web. [Ver demo](#).

Continuación ...

Compartir

Me gusta Registrarse para ver qué les gusta a tus amigos.

Twitter 0

0 comentarios Tags: anti malware, anti spyware, networkers community, novirusthanks, scanurls, urlvoid, webmaster

[Leer siguientes »](#)

## Networkers

Webmasters

14 Jul 2012

### Servicios PING

Escrito por: [José María Amenós Vidal](#) el 14 Jul 2012 - [URL Permanente](#)

Watchmouse ofrece información actualizada sobre la disponibilidad de su sitio web mediante comprobaciones de calidad continuas de la accesibilidad de su servidor web, 24 horas al día, los 7 días de la semana, desde distintos puntos del planeta. Un servicio de control de sitios web de Nimsoft Cloud Monitor. [Ver / descargar](#).

Confirmada la buena disponibilidad, accesibilidad y funcionamiento de nuestro blog os ofrecemos varios sitios para hacer PING (Packet Internet Groper) con vuestro feed atom/rss/xml en la red.

1. <http://ping.bitacoras.com>
2. <http://rpc.twingly.com>
3. <http://rpc.weblogs.com/RPC2>
4. <http://blogsearch.google.com/pingRPC2>
5. <http://ping.bloggs.com>
6. <http://ping.feedburner.com>
7. <http://pingoat.com/goat/RPC2>
8. <http://rpc.pingomatic.com>
- (...)

Estas direcciones electrónicas se añaden en la opción correspondiente de configuración del panel de control de administración del blog disponible para insertar la lista de servicios PING separados por comas (por ej) en Simple PHP Blog).

De este modo, cada vez que publiquéis o editéis un post este se actualizará en los sitios con los que hacéis PINGs. Os recomendamos que simultáneamente registréis previamente vuestro blog en cada una de dichas plataformas - bitacoras.com, twingly.com, weblogs.com, google.com, blo.gs, feedburner.com, pingoat.com, pingomatic.com, etc ...

Compartir     

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 0

 0 comentarios Tags: [sprngblog](#), [nimsoft](#), [watchmouse](#), [bitacoras](#), [twingly](#), [weblogs](#), [google](#), [feedburner](#), [pingoat](#), [pingomatic](#), [blo](#)

25 Jun 2012

### HOAX : Ex-hacker en el Vaticano

Escrito por: [José María Amenós Vidal](#) el 25 Jun 2012 - [URL Permanente](#)

Declaraciones del portavoz de la Santa Sede atribuyen al diario italiano La Repubblica la noticia sobre el ex-hacker en el Vaticano que en un primer momento tuvo su difusión en la RNV - Radio Nacional de Venezuela, así como en el Canal TV - Russia Today - RT ...

Sus palabras : "Me quedé sorprendido. Realicé verificaciones en la Gobernación, la Gendarmería y la Secretaría de Estado y no encontré absolutamente nada".

#### Tango down y Anonymous.

Las filtraciones que han dado origen al caso "Vatileaks" empezaron de forma simultánea al plan de acciones de Anonymous contra las páginas oficiales del estado Vaticano que se cifieron a varios ataques ...

Continuación ...

Para más información : HOAX - Un ejemplo de la teoría del rumor en Internet. [Ver / descargar](#).

Compartir     

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 0

 0 comentarios Tags: [anti malware](#), [stopthehacker](#), [rnv](#), [rt](#), [hoax](#)

31 May 2012

### Certificado de Legalidad

Escrito por: [Carmen Martínez Ibáñez](#) el 31 May 2012 - [URL Permanente](#)

 **internetLegal** Es para informarles que cumplimentadas las gestiones pertinentes para la obtención del certificado de legalidad, se nos ha otorgado el sello de Internet Legal que certifica el cumplimiento de la legislación española en materia de protección de datos y comercio electrónico en la web: [estrategia.info](http://estrategia.info), [psicologoscatolicos.org](http://psicologoscatolicos.org) e [infocath.com](http://infocath.com)

Los pasos a seguir han sido los siguientes :

1. Inscripción en InternetLegal. Nº de certificado. S20120512142038, S20120512151228 y S20120512152835
2. Aviso legal lssi.
3. Ficheros agpd (base de datos),

#### AUDITORIA IL

Estos sitios web pertenecen a José María Amenós Vidal con NIF: 35049269Y, domiciliados en: c/ Museo, 26 - 1-1 08912 Badalona en la provincia de Barcelona, con teléfono 934644867.

Para verificar esta información se han solicitado los siguientes documentos acreditativos:

- N.I.F. / C.I.F.
- Registro del dominio.
- Modelo 036 de alta en actividades económicas.
- Estos sitios web SI solicitan datos personales mediante formularios.
- Los sitios web que solicitan datos personales mediante formularios, han de cumplir la LOPD (Ley Orgánica de Protección de Datos).
- Hemos verificado la inscripción del fichero en la Agencia de Protección de Datos.
- Hemos verificado la existencia en los sitios web de los avisos legales oportunos al solicitar datos personales y hemos comprobado que existe la información suficiente para que el titular de los datos pueda ejercitar su derecho de cancelación o rectificación mediante escrito dirigido al responsable del fichero de la entidad.
- Estos sitios web NO realizan comercio electrónico.

Descripción de la empresa

UN GRUPO DE EDICIONES Y MEDIOS ELECTRONICOS O DIGITALES QUE DISPONE DE UN SERVICIO DE CONSULTAS E INFORMACION CATOLICA PARA HISPANOAMERICA Y DE UN PROGRAMA DE FORMACION O EQUIPO DE DOCCENCIA E INVESTIGACION CON ESPRITU EUCUMENICO DIRIGIDO A LAICOS/AS, RELIGIOSO/AS O SACERDOTES FIELES AL MAGISTERIO PONTIFICIO Y EL SANTO PADRE.

Compartir     

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 0

 0 comentarios Tags: [internet legal](#), [networkers community](#), [il](#), [lssi](#), [lssice](#), [webmaster](#), [littina](#), [lopd](#)

30 May 2012

### Copyscape e informes de transparencia de Google

Escrito por: [José María Amenós Vidal](#) el 30 May 2012 - [URL Permanente](#)

En los informes de transparencia que Google ha comenzado a hacer públicos, con el fin de que los usuarios en internet sean informados de las páginas web que han sido denunciadas para suprimirlas del índice del buscador porque por una razón u otra han vulnerado la ley (lssice, lopy, etc ...), o infringido los derechos de autor (copyright).

Os comunicamos que los dominios vinculados a nuestro servicio de información católica para hispanoamérica ([estrategia.info](http://estrategia.info), [psicologoscatolicos.org](http://psicologoscatolicos.org) e [infocath.com](http://infocath.com)) no se hallan entre las 105.928 direcciones electrónicas que constituyen todos los datos disponibles (25 mayo 2012). [Ver / descargar](#).

Os aconsejamos y recomendamos : COPYSCAPE

Compartir     

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 0

 0 comentarios Tags: [networkers community](#), [copyscape](#), [google](#), [webmaster](#), [copyright](#), [lssice](#), [lssi](#), [lopd](#)

27 Abr 2012

### Stop The Hacker : Blacklist Monitoring

Escrito por: [José María Amenós Vidal](#) el 27 Abr 2012 - [URL Permanente](#)



StopTheHacker es una utilidad para webmasters que te ofrece el mismo servicio que tiempo atrás Dasient WAM - Web Anti-Malware nos brindaba de forma gratuita, por esta razón os lo recomendamos. [Pulse aquí](#).

Se trata de una herramienta en línea para la monitorización de un espacio web que nos sirve de aviso de posibles inyecciones de malware en nuestro host o servidor, teniendo de este modo vigilado las 24 h. los 365 días del año nuestro sitio en internet. [Ver / descargar](#).

#### Formulario de registro.

Después de inscribirnos y daros de alta en la plataforma, podréis acceder al panel de control en que podéis incluir hasta al menos 3 urls o direcciones electrónicas para hacer su seguimiento.

#### Informes periódicos.

La información que nos envía el sistema por defecto, es un detalle sobre nuestro dominio inscrito y si ha pasado a engrosar o no la lista negra de espacios que entrañan un riesgo de seguridad para la red.

En resumen, el tipo de datos que se facilita en modo automático detalla si sus urls siguen siendo seguras o forman parte de una lista negra, al modo de Google Safe Browsing + Malware Domain List.

Compartir     

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 0

 0 comentarios Tags: [malware domain list](#), [anti malware](#), [webmaster](#), [stopthehacker](#), [dasient](#), [google](#)

08 Abr 2012

### Wireless Network Watcher

Escrito por: [José María Amenós Vidal](#) el 08 Abr 2012 - [URL Permanente](#)

WNW es una utilidad de monitorización que escanea la WIFI o red inalámbrica y muestra una lista de todos los equipos que están conectados. La información viene detallada por dirección IP del dispositivo, nombre del equipo, MAC del adaptador, fabricante de la tarjeta de red u otros datos con la posibilidad de exportarlos en varios formatos (html, xml, csv o txt).

Esta aplicación funciona con Windows 2000, XP, Server 2003/08, Vista y 7, y rastrea las conexiones activas, por lo que excepcionalmente también puede usarse para examinar una línea por cable. se instala mediante archivo ejecutable y realiza la detección automática de routers, ordenadores, etc ...

IP Address	Device Name	MAC Address	Network Adapter Company	Device Informa
192.168.0.1	MYCOMP2	00-03-47-F1-...	Intel Corporation	
192.168.0.11	new1	00-19-D1-67-...	Intel Corporation	Your Computer
192.168.0.15	WIN7-PC	08-00-27-3C-...	CADMIUS COMPUTER SYSTEMS	
192.168.0.10	NETBOOK	6C-62-6D-10-...	Micro-Star INTL CO., LTD	
192.168.0.254		00-25-9C-64-...	Cisco-Linksys, LLC	Your Router

WNWWatcher dispone de configuración de alertas, mediante el menú de opciones y el marcapag automático de "beep on new device" y "background scan" el programa de escaneado nos avisará cada vez que advierta la conexión de un equipo.

Nirsoft detenta los derechos de Wireless Network Watcher y lo distribuye con licencia freeware, de modo que se autoriza su libre distribución siempre y cuando no se haga un uso fraudulento del mismo ni con fines comerciales. [Ver / descargar](#).

Compartir     

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 0

 0 comentarios Tags: [nirsoft](#), [wifi](#), [windows](#), [ip](#), [os](#)

07 Abr 2012

### WWF : una nueva extensión de archivo en formato ecológico

Escrito por: [Carmen Martínez Ibáñez](#) el 07 Abr 2012 - [URL Permanente](#)



Un fichero WWF es un PDF que no se puede imprimir. De esta sencilla manera, se evita la impresión innecesaria de documentos, lo que beneficia al medio ambiente.

Evitar la sobreexplotación de las plantaciones de árboles para obtener pasta de papel está en tus manos. Decide por ti mismo qué documentos no precisan ser impresos y guárdalos en formato WWF.

Usa este plugin para abrir y guardar archivos, disponible para Mac OS X 10.4+ y Windows XP o superior. [Ver / descargar](#).

WWF es una marca registrada de WWF International - World Wide Fund for Nature para el desarrollo de software con sede en Gland (Suiza).

**Guía del usuario.**

- Condiciones de uso.
- Preguntas frecuentes.



Compartir     

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 0

 0 comentarios Tags: [wwf](#)

13 Mar 2012

### Tango Down y Anonymous

Escrito por: [José María Amenós Vidal](#) el 13 Mar 2012 - [URL Permanente](#)

De forma simultánea Anonymous hackea Panda y establece un plan de acciones contra las páginas oficiales del estado Vaticano que se cifien hasta el momento a varios ataques perpetrados desde primeros de marzo.

En terminología militar el concepto "Tango Down" se refiere a objetivo abatido, con este fin los hackers pretenden bloquear el servidor o al menos interrumpir su servicio. Sin embargo, también ha trascendido que las bases de datos son vulneradas y se inyecta código malicioso.

Por esta razón, se han hecho públicas informaciones que hablan tanto de la afectación de subdominios de Panda a nivel global, así como de funcionarios y autoridades vaticanas como el coordinador del equipo web, Pietro Cozzo, el administrador de sistemas y jefe de proyectos, Massimiliano Di Bello, o el desarrollador de software, Fabio Valerio.

**Si entre la piratería informática se aplica la máxima de que la mejor defensa es el ataque, en el ámbito de la seguridad en internet, no hay mejor defensa que prevenir un ataque.**

De este modo, y en base a experiencia adquirida contra códigos malintencionados que han sido creados por grupos cibercriminales que tienen su origen en servidores remotos de origen desconocido con el propósito de permitir malware en sitios legítimos, es decir, ante la imposibilidad de detener a las personas físicas que son autores materiales de los ataques, el único modo de actuar es establecer las contramedidas adecuadas que permitan detener posibles intrusiones.

Con este propósito, los consejos y aplicaciones de nuestra metodología WAM - Web Anti-Malware.

- [Importante aviso para webmasters \(...\)](#)
- [Libro electrónico en biblioteca universitaria \(paper\)](#)
- [PulpoLab : Cómo proteger de software malicioso la web \(abstract\)](#)

Compartir     

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 0

 0 comentarios Tags: [anti malware](#), [networkers community](#), [webmaster](#), [panda](#)

07 Mar 2012

### Anonymous hackea Panda

Escrito por: [José María Amenós Vidal](#) el 07 Mar 2012 - [URL Permanente](#)

El grupo de hackers anónimo que conforman la mayor organización de piratería informática en todo el mundo, ha hackeado docenas de subdominios de la compañía PANDA dedicada a la creación de software de seguridad. A continuación pasamos a detallar las direcciones que se han visto afectadas.

1. [cybercrime.pandasecurity.com](http://cybercrime.pandasecurity.com)
2. [antivirus-offers.pandasecurity.com](http://antivirus-offers.pandasecurity.com)
3. [blog.cloudantivirus.com](http://blog.cloudantivirus.com)
4. [cloudofficeprotection.pandasecurity.com](http://cloudofficeprotection.pandasecurity.com)
5. [cloud.pandasecurity.com](http://cloud.pandasecurity.com)
6. [cloudpartnercenter.pandasecurity.com](http://cloudpartnercenter.pandasecurity.com)
7. [cloudprotectionbeta.pandasecurity.com](http://cloudprotectionbeta.pandasecurity.com)
8. [tg.gz](http://tg.gz)
9. [facebookfriends.pandasecurity.com](http://facebookfriends.pandasecurity.com)
10. [forgetsecurity.co.uk](http://forgetsecurity.co.uk)
11. [forgetsecurity.co.za](http://forgetsecurity.co.za)
12. [forgetsecurity.es](http://forgetsecurity.es)
13. [go.pandasecurity.com](http://go.pandasecurity.com)
14. [info.pandasecurity.com](http://info.pandasecurity.com)
15. [information.pandasecurity.com](http://information.pandasecurity.com)
16. [lavuelta.pandasecurity.com](http://lavuelta.pandasecurity.com)
17. [maintenance.pandasecurity.com](http://maintenance.pandasecurity.com)
18. [momentos.pandasecurity.com](http://momentos.pandasecurity.com)
19. [ordersteuning.pandasecurity.com](http://ordersteuning.pandasecurity.com)
20. [panda.competition.pandasecurity.com](http://panda.competition.pandasecurity.com)
21. [pandalabs.pandasecurity.com](http://pandalabs.pandasecurity.com)
22. [prensa.pandasecurity.com](http://prensa.pandasecurity.com)
23. [press.pandasecurity.com](http://press.pandasecurity.com)
24. [promo.pandasecurity.com](http://promo.pandasecurity.com)
25. [protectyourfamily.pandasecurity.com](http://protectyourfamily.pandasecurity.com)
26. [research.pandasecurity.com](http://research.pandasecurity.com)
27. [securitythecloud.pandasecurity.com](http://securitythecloud.pandasecurity.com)
28. [serviciospro.pandasecurity.com](http://serviciospro.pandasecurity.com)
29. [servicos.pandasecurity.com](http://servicos.pandasecurity.com)
30. [suporte.pandasecurity.com](http://suporte.pandasecurity.com)
31. [techcenter.pandasecurity.com](http://techcenter.pandasecurity.com)
32. [uninstall.cloudantivirus.com](http://uninstall.cloudantivirus.com)
33. [wiki.cloudantivirus.com](http://wiki.cloudantivirus.com)
34. [www.cnccs.es](http://www.cnccs.es)
35. [www.forgetsecurity.de](http://www.forgetsecurity.de)
36. [www.forgetsecurity.se](http://www.forgetsecurity.se)

Esta empresa que se ha distinguido en el pasado por sus colaboraciones para desmantelar redes de ordenadores (botnets, zombiebots, spambots, etc ...) cautivos bajo el control remoto de malware usado por grupos cibercriminales (ver declaraciones de Panda Labs sobre la botnet que afectó a 13 millones de usuarios en 190 países y 31.901 ciudades) ha sido víctima en esta ocasión de Anonymous.

#### Recomendaciones para usuarios y webmasters.

Ante una situación tan inusual observando la vulnerabilidad de un grupo empresarial de estas características, procedemos a desvelar como tenemos blindados nuestros PCs, cambiando la tecnología de Norton Internet Security. Para más información [pulse aquí](#).

Es decir, además del antivirus de Symantec y de instalar Panda Cloud, procedimos a prevenir posibles incidencias implementando los siguientes programas de refuerzo : Microsoft Security Essentials, AVG Technologies, Browser Guard y RuBotted de Trend Micro.

Compartir     

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 0

 0 comentarios Tags: [trend micro](#), [avg technologies](#), [networkers community](#), [anti malware](#), [anti spyware](#), [panda](#), [norton](#), [symantec](#), [microsoft](#), [webmaster](#), [windows](#)

## Networkers

Webmasters

01 Ene 2012

### QR Codes

Escrito por: [José María Aménos Vidal](#) el 01 Ene 2012 - [URL Permanente](#)

En la infinidad de aplicaciones para móviles de nueva generación que contienen lectores de códigos QR (Quick Response) para múltiples plataformas, hemos seleccionado un entorno web que nos permite a través del PC conocer el funcionamiento de este método de codificación cuyo uso generalizado se está extendiendo cada vez más por la red.

JS - Janones Sistemas es un portal brasileño que dispone de un **generador / codificador y lector / decodificador** de QR Codes.



A modo de ejemplo, utilizaremos un gráfico ya generado, de modo que si introducimos su url:  
<http://www.feedage.com/qrgen.php?feed=15374535>  
 El lector de códigos comprobará su decodificación que equivale al feed:  
<http://estrategia.info/fpc/rss.php>

El principio en el que se basa esta nueva funcionalidad es similar al código de barras, considerando la actual capacidad de leer imágenes a través de un escaneado fotográfico, o bien con una webcam desde el ordenador o cámara digital del teléfono móvil con conexión a internet, de manera que el dispositivo sindicado disponiendo de un lector de códigos QR nos mostrará su información, en el caso señalado el agregador de noticias de un sitio web.

Compartir

Me gusta Regístrate para ver qué les gusta a tus amigos.

**Twitter** 0

0 comentarios Tags: janones sistemas, qr, feedage

24 Dic 2011

### Is the Web Safe

Escrito por: [Carmen Martínez Ibañez](#) el 24 Dic 2011 - [URL Permanente](#)

#### Website Security & Safety Report



**IsTheWebSafe.com** es un directorio de sitios en internet relativamente nuevo que ya dispone de cientos de miles de espacios indexados con el fin de ofrecer un medio de información válido y fiable en cuanto a seguridad de navegación por la red a través de un servicio gratuito de búsqueda de cualquier informe de una web. [Pulse aquí.](#)

Para inspeccionar una página electrónica, sólo tiene que utilizar su motor de rastreo, tecleando cualquier nombre de dominio en la barra del buscador. Se trata de una herramienta de análisis complejo que destaca por su sencillez y rapidez, ofrece evaluaciones de resultados básicos sobre el dominio, servidor u otras opciones, se centra en la calidad (quality), confianza (confidence) y utilidad (usefulness), control parental (child safety), software malicioso (malware) y fraude (phishing), facilitando un porcentaje (global score) como indicador de nivel entre 0 - 100 %. Ejemplo : [Ver / descargar.](#)

Compartir

Me gusta Regístrate para ver qué les gusta a tus amigos.

**Twitter** 0

0 comentarios Tags: anti malware, anti spyware, child safety, control parental, is the web safe, networkers community, webmaster

22 Dic 2011

### SEO + Quality Validator

Escrito por: [José María Aménos Vidal](#) el 22 Dic 2011 - [URL Permanente](#)

#### Test Website Analysis Report.



**SEO.com.** Es el primer portal de expertos especializados en Search Engine Optimization (SEO) y pone a disposición de los usuarios un método de evaluación eficaz y capaz de orientarnos sobre cómo se está desempeñando nuestro sitio en la red y que aspectos más importantes son susceptibles de mejorar en cuanto a posicionamiento en los principales buscadores : Google, Bing, Yahoo u otros.

Para determinar su clasificación en línea, los motores de búsqueda no sólo escanean el contenido de su página electrónica, sino también la estructura. Rellenando el siguiente [formulario](#) de forma automática serán escaneados tanto los contenidos como sus codificaciones para descubrir las áreas de mejora que puede implementar con el fin de optimizar su presencia en internet. Ejemplo : [Ver / descargar.](#)



**Qualidator.com.** Mide los principales parámetros de un espacio en la red que definen su éxito en internet, también en términos económicos, lleva el potencial de un sitio web a su vida.

Se trata de 60-70 tests automatizados sobre los aspectos básicos de usabilidad, accesibilidad, optimización para motores y calidad técnica. Introduzca la URL (Uniform Resource Locator) o dirección electrónica de un dominio en la [herramienta de análisis](#). La prueba tiene una duración de 1-5 minutos, según el proceso de datos y la carga del servidor. Ejemplo: [Ver / descargar.](#)

Compartir

Me gusta Regístrate para ver qué les gusta a tus amigos.

**Twitter** 0

0 comentarios Tags: qualidator, seo, webmaster, google, alexa, yahoo, bing

15 Dic 2011

### Domain Name System Validation

Escrito por: [Carmen Martínez Ibañez](#) el 15 Dic 2011 - [URL Permanente](#)

#### Encuentra rápidamente cualquier problema en el DNS.

DNSValidation.com es una herramienta en línea que comprueba los servidores web de su dominio y correo para descubrir posibles problemas, generando un informe con validaciones, avisos o errores y explicaciones para solucionarlos. [Pulse aquí.](#)

Es un proyecto de Vitalie Cherpac, y desde 2008 su objetivo es crear una herramienta gratuita de control DNS usando OSS (Open Source Software), y desde entonces, está constantemente mejorando su soporte, con más de 50 tests o pruebas en un sólo proceso: análisis, sin necesidad de utilizar otros recursos o líneas de comando, comprueba el nombre del servidor y verifica sus múltiples parámetros con el fin de señalar entre 0-10 el estado de su Domain Name System.

Un ejemplo de DNS Validation. [Ver / descargar.](#)

Compartir

Me gusta Regístrate para ver qué les gusta a tus amigos.

**Twitter** 0

0 comentarios Tags: dns validation, osi, webmaster

05 Dic 2011

### Open Website Reputation

Escrito por: [Carmen Martínez Ibañez](#) el 05 Dic 2011 - [URL Permanente](#)

#### Reputación Web contra el fraude y malware.



Webutation.net hace que la World Wide Web sea un lugar más seguro. Se trata de un proyecto público y abierto sobre la reputación de cualquier sitio en internet. Chequea las páginas electrónicas con pruebas contra spam o correo no deseado, phishing o estafas usuales, etc ... realizando consultas en línea con tecnología de escaneado inteligente y en tiempo real en base a:

- Google SafeBrowsing contra el software malicioso y el fraude (se actualiza cada media hora).
- Website Antivirus que escanea los sitios contra el adware (ventanas emergentes), spyware (enlaces salientes) y virus.
- WOT (Web of Trust) que recoge comentarios de los usuarios y la experiencia de los clientes sobre sitios u otros recursos.
- G-Rated / Child Safety analiza el grado de protección o control parental.

En general, es un potente analizador que alcanza a ofrecer un porcentaje ponderado de varias herramientas al uso en seguridad informática y que lo convierten en un poderoso rastreador de vulnerabilidades en la red.

Para más información : Un ejemplo de análisis de reputación web. [Ver / descargar.](#)

Compartir

Me gusta Regístrate para ver qué les gusta a tus amigos.

**Twitter** 0

0 comentarios Tags: child safety, control parental, g rated, anti malware, anti spyware, webutation, google, webmaster, wot

03 Dic 2011

### Website Safety Check

Escrito por: [José María Aménos Vidal](#) el 03 Dic 2011 - [URL Permanente](#)

#### Control de seguridad de cualquier sitio web.



Se ha desarrollado el proyecto en línea de Surf Safely como contribución para el mantenimiento de la red como un lugar seguro para los usuarios de Internet. [Pulse aquí.](#)

Website Safety Check analiza un sitio web para su seguridad y trata de ofrecer resultados razonablemente precisos mediante la combinación de diversos datos de diferentes fuentes de buena reputación, junto con la realización de una investigación sobre la seguridad de los sitios con el fin de dar una puntuación global en porcentajes para orientación del usuario.

La comprobación de sitios es muy fácil, basta con introducir en la orientación de análisis el dominio del que desea saber su grado de fiabilidad y los resultados se obtienen de inmediato. Esta herramienta de apoyo es gratuita, rápida y fiable.

Para más información : Un ejemplo de chequeo. [Ver / descargar.](#)

Compartir

Me gusta Regístrate para ver qué les gusta a tus amigos.

**Twitter** 0

0 comentarios Tags: anti malware, anti spyware, website safety check, surf safely, webmaster

05 Nov 2011

### SEO Score : Site Trail + Ustats + Website Informer

Escrito por: [José María Aménos Vidal](#) el 05 Nov 2011 - [URL Permanente](#)

Con los cambios recientes que ha experimentado el algoritmo de Google para indexar en sus directorios los contenidos en su motor de búsquedas con el fin principal de penalizar a los spammers y beneficiar los contenidos actualizados por webmasters, nos han llevado en [estrategia.info](#) a medir el SEO Score a través de Site Trail y los índices de progresión estadística en relación a las visitas y páginas consultadas mediante Ustats y Website Informer.

De esta forma, tras estas primeras consideraciones facilitamos los resultados preliminares que reflejan la mejora en la actividad que se desprende de la labor de optimización en cuanto a contenidos, códigos y cumplimiento de las normas certificadas por QWEB relativos a SEO - Search Engine Optimization y la evaluación de datos estadísticos en cuanto a usuarios actuales en nuestra plataforma de Internet.

- El SEO Score medido por Site Trail oscila entre el 60-70 % para el Blog y CMS.



- Ustats según la última actualización nos indica una media aritmética, con 86 visitas y 430 páginas vistas por hora. [Ver / descargar.](#)
- Website Informer que realiza estimaciones comparativas con **Alexa**, arroja un balance entre 1.458 - 2.764 visitas y 36.446 - 63.563 páginas vistas por día basadas en el CMS y Blog, respectivamente.

Compartir

Me gusta Regístrate para ver qué les gusta a tus amigos.

**Twitter** 0

0 comentarios Tags: site trail, informer technologies, google, alexa, webmaster, seo, ustats, qweb

21 Oct 2011

### Bloquear los anuncios de Google

Escrito por: [Carmen Martínez Ibañez](#) el 21 Oct 2011 - [URL Permanente](#)



Ante la interrogación de diseñar un buscador adecuado a las necesidades de una web que no dispone de motor de búsquedas, como por ejemplo, cuando usamos Podcast Generator, una solución open source para la publicación de podcasts, que cumple muy bien con su función, y que tras sopesar la opción de búsqueda personalizada de Google, hemos considerado sigue siendo el motor más adecuado para nuestros requerimientos, nos encontramos con una dificultad y es la presencia de anuncios esponsorizados que son un problema para los webmasters y usuarios, en cuanto publicita contenidos a nuestra voluntad.

No obstante, para suprimir esta publicidad, Google Site Search hace abonar un precio inicial de 100 dólares al año para eliminarla de los resultados. Sin embargo, existen otras soluciones, y por esta razón, hablamos hoy de Simple Adblock para Internet Explorer (IE), se trata de una extensión para el explorador, de sencillo uso e instalación, que bloquea la publicidad, con el correspondiente ahorro económico y de otras molestias.

Para su mejor entendimiento, hemos de fijarnos en el siguiente sitio en Internet, que a pie de página electrónica hemos aplicado los principios mencionados. [Pulse aquí.](#)

En primer lugar, creamos el buscador personalizado y copiamos el código por defecto que nos facilita Google en nuestro espacio. [Ver / descargar.](#)

Posteriormente, situado en su lugar hacemos la prueba insertando el término en la casilla correspondiente y pulsamos buscar, apareciendo entonces la propaganda y en segundo plano los resultados.

De este modo, si procedemos a instalar en IE la aplicación de Simple Adblock de manera que quede habilitada su funcionalidad en el navegador conseguiremos que la cadena de búsqueda aparezca sin anuncios esponsorizados. [Ver / descargar.](#)

Compartir

Me gusta Regístrate para ver qué les gusta a tus amigos.

**Twitter** 0

0 comentarios Tags: podcast generator, internet explorer, simple adblock, google, webmaster, osi

16 Oct 2011

### Browser Guard + Safe Browsing

Escrito por: [José María Aménos Vidal](#) el 16 Oct 2011 - [URL Permanente](#)

En la intención de ofrecer nuevas herramientas de protección para el usuario y webmaster, os proponemos una combinación que hemos venido utilizando durante algún tiempo y nos está resultando muy provechosa ante posibles amenazas a infecciones.

En esta ocasión nos centraremos en una multiplicidad de estrategias enfocadas a salvaguardar tanto nuestro explorador que es el más vulnerable al código malicioso, software malintencionado o producido por malware, así como a evitar los peligros que entraña la red en cuanto a sitios susceptibles de comprometer nuestra seguridad.

Sin embargo, estas opciones que os planteamos serán complementarias a los antivirus, cortafuegos y demás recursos instalados en el PC que garantizan nuestra defensa ante posibles intrusiones, es decir, pretenden ampliar la gama de utilidades que nos permitirán optimizar la prevención de riesgos.

#### 1. Safe Browsing



Utilice la experiencia de una herramienta de navegación segura. Safe Browsing de Web of Trust es un simple marcador que nos indica la confianza de los hipervínculos dinámicos que aparecen por ejemplo cuando consultamos los resultados en un motor de búsqueda, abrimos un mensaje de correo electrónico que contiene enlaces a otras páginas, etc ...

Se trata de un sistema que se instala con facilidad en los navegadores Internet Explorer, Mozilla Firefox, Google Chrome, Safari u Opera, y sirve a la función de indicar con un círculo de colores que oscila del verde, ámbar y rojo, como si fuera un semáforo, aquellas webs que deberíamos o no visitar en base a una evaluación sobre parámetros de confiabilidad, fiabilidad, privacidad y control parental. [Ver / descargar.](#)

#### 2. Browser Guard



Proteja de forma activa su explorador contra amenazas de Internet. Browser Guard de Trend Micro previene la vulnerabilidad y protege contra JavaScript malintencionado, usa heurística avanzada y tecnologías de emulación, se actualiza de forma rápida y permanente, proporciona la tecnología más segura y avanzada en cuanto a mejoras en la detección de troyanos web y seguimiento de las cadenas de infecciones. [Ver / descargar.](#)

Observaciones : Aconsejamos que junto a la instalación de Browser Guard implementen la aplicación de Rubotted que les indicará si su ordenador encuentra o ha caído cautivo en una botnet, monitorizará y vigilará su PC para que no se convierta en un zombi. [Ver / descargar.](#)

Sin embargo para su uso resulta recomendable utilizar HouseCall + Smart Response Network como les indicamos en una anterior noticia. [Pulse aquí.](#)

Compartir

Me gusta Regístrate para ver qué les gusta a tus amigos.

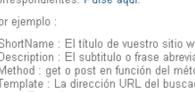
**Twitter** 0

0 comentarios Tags: internet explorer, anti malware, anti spyware, mozilla firefox, trend micro, web of trust, windows, safari, opera, google, wot, webmaster

12 Oct 2011

### Open Search Plugin

Escrito por: [José María Aménos Vidal](#) el 12 Oct 2011 - [URL Permanente](#)



Hoy os traemos un ejemplo de código optimizado que os puede ser de mucha utilidad a la hora de buscar y encontrar contenidos en vuestro sitio en la red desde el navegador.

Se trata de un plugin Open Source que se instala en el explorador utilizando el buscador de vuestra página electrónica. De esta manera, disponiendo de esta utilidad, herramienta o aplicación os será posible hacer consultas en vuestra web desde Internet Explorer, Mozilla Firefox, Google

Chrome, Netscape ...

En primer lugar, a modo de ejemplo se trata de elaborar un fichero de nombres y formato opensearch.xml con el siguiente código fuente en el que debes sustituir los diferentes valores en función de los datos correspondientes. [Pulse aquí.](#)

Por ejemplo :

- ShortName : El título de vuestro sitio web.
- Description : El subtítulo o frase abreviada que os define en la red.
- Method : get o post en función del método que usa vuestro servidor.
- Template : La dirección URL del buscador de vuestro sitio en internet (es importante añadirle {searchTerms}).
- Image : El favicon en formato ico de dimensiones 16 x 16 px.
- Developer : El nombre del desarrollador.
- Encoding : La codificación se puede mantener UTF-8.
- Search Form : El dominio principal.

Si nos fijamos sobre el resto de propiedades es importante ubicar opensearch.xml en el directorio principal del dominio y especificar la ruta de acceso al fichero cargando en el servidor.

Finalmente, podemos establecer un enlace desde el que cualquier usuario puede instalar el plugin como nuevo proveedor o motor de búsqueda del navegador mediante la ejecución de un javascript cuya fuente de código html es el siguiente :

```
<A href=
<A href=javascript:window.external.AddSearchProvider('http://estrategia.info/opensearch.xml')>Instalar</A>
En nuestro caso hemos optado por insertar un equivalente más elaborado en php. Ver / descargar.
echo"<p align=center><a
href=javascript:window.external.AddSearchProvider('http://estrategia.info/opensearch.xml')><img
src=http://estrategia.info/fpc/images/opensearch.png border=0></a></p>";"
```

Compartir

Me gusta Regístrate para ver qué les gusta a tus amigos.

**Twitter** 0

0 comentarios Tags: mozilla firefox, internet explorer, networkers community, google, webmaster, addoursearch, java, netscape, osi, spqblog, toolbar, windows

[« Leer anteriores](#)

# Networkers

Webmasters

06 Oct 2011

## Website Analysis : WooRank + AboutUs + SiteIntel

Escrito por: [Carmen Martínez Ibáñez](#) el 08 Oct 2011 - [URL Permanente](#)



Después de unos meses de configurar los diferentes parámetros que conforman el dominio estrategia.info y conseguir certificar para buscadores por QWEB, se aprecian los primeros resultados en cuanto a su mejora en posicionamiento.

Para ello, observamos como indicadores válidos de esta operación realizada con el fin de ofrecer un sitio en la red que cumpla con los mejores estándares de calidad, los siguientes datos obtenidos del análisis de contenidos generados por nuestra comunidad que han sido testados por varios de los siguientes proveedores en Internet.

OFF-PAGE:

1. Web Positer - Search Marketing.
- ON-LINE
1. Site Intel - know Your Competition.
2. About US - We know the Web.
3. Woo Rank - Website Analysis Tool.

En general los valores de ALEXA - The Web Information Company expresan este esfuerzo realizado en cuanto a SEO - Search Engine Optimization.

Compartir

Me gusta

Regístrate para ver qué les gusta a tus amigos.

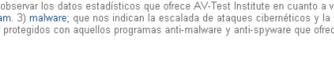
Twitter

0 comentarios Tags: alexa, seo, siteintel, aboutus, worank, qweb, weposter

26 Sep 2011

## AV Test Institute

Escrito por: [Carmen Martínez Ibáñez](#) el 26 Sep 2011 - [URL Permanente](#)



Desde Networkers Community mencionamos varios productos anti-virus por su eficacia, y revisando los datos de certificación que ofrece el consultor independiente en materia de seguridad informática AV-Test.org según los últimos listados públicos que ofrece por puntuación del 1 al 6 con el fin de valorar los diferentes grados de efectividad, hemos comprobado que las versiones gratuitas que os hemos recomendado tanto de AVG, Kaspersky, Microsoft, Panda, Symantec y Trend Micro (por orden alfabético), que son los aconsejados en nuestras informaciones se confirman que disponen de mayores puntuaciones en cuanto a sus modalidades en Internet. Ver / descargar.

Os emplazamos a observar los datos estadísticos que ofrece AV-Test Institute en alguna de varios parámetros : 1) updates. 2) spam. 3) malware, que nos indican la escalada de ataques cibernéticos y la creciente necesidad de estar protegidos con aquellos programas anti-malware y anti-spyware que ofrecen las mejores prestaciones.

Compartir

Me gusta

Regístrate para ver qué les gusta a tus amigos.

Twitter

0 comentarios Tags: avg technologies, av test, anti malware, anti spyware, networkers community, kaspersky, microsoft, panda, symantec, webmaster, norton

23 Sep 2011

## II Congreso RIAL

Escrito por: [José María Amador Vidal](#) el 23 Sep 2011 - [URL Permanente](#)



Con el fin de que nuestra metodología WAM - Web Anti-Malware tenga el máximo grado de difusión en el ámbito eclesial que más nos interesa, la hemos inscrito en la modalidad virtual del II Congreso RIAL - Red Informática de la Iglesia en América Latina (Santiago de Chile, 17-19 octubre 2011). Iglesia y Cultura Digital - "Nuevos horizontes para la misión eclesial". Ver / descargar.

Un criterio importante para la participación en el Congreso consiste en ofrecer alguna reflexión, experiencia o aportación a las temáticas del encuentro. Esta condición apunta a animar una participación activa desde el principio, y abre la posibilidad de iniciar una reflexión conjunta que culmine en el encuentro.

Están convocados los Obispos Presidentes y los ejecutivos/as de comunicación y RIAL de las Conferencias Episcopales de América Latina, además de responsables de medios católicos en formato digital, académicos e impulsores de instituciones con experiencias válidas en este campo. En los siguientes enlaces se ofrece toda la información.

- Solicitudes de participación.
- Ponentes y panelistas.
- Aportaciones y Comunicaciones.

El proceso de elaboración de nuestra propuesta se basa en la experiencia adquirida del 25 de junio al 3 de septiembre del 2009 y fechas posteriores, e incluso a causa del último ataque sufrido con intento de intrusión en nuestro PC, Web y Servidor FTP en días recientes, del 6 al 8 de septiembre del 2011, que detallamos en el siguiente hipervínculo dinámico. Pulse aquí:

Los datos que constan en el programa congresual sobre nuestra comunicación técnica se detallan a continuación.

- Grupo de trabajo : Cultura digital: características y mutaciones.
- Categoría : Seguridad, privacidad y riesgos en Internet.
- Autor : José María Amador Vidal
- e-mail : info@psicologoscatolicos.org
- Título : Internet y Seguridad.

Continuación...

Compartir

Me gusta

Regístrate para ver qué les gusta a tus amigos.

Twitter

0 comentarios Tags: hazte or, networkers community, anti malware, rial, webmaster

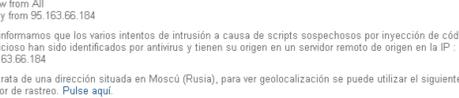
12 Sep 2011

## QWeb.es : Resultado de la revisión y sello de certificación

Escrito por: [Carmen Martínez Ibáñez](#) el 12 Sep 2011 - [URL Permanente](#)

Tras realizar la auditoría de la página web para la que solicitamos la concesión del Certificado de Adecuación a BUSCADORES, nos complace comunicarnos que [www.estrategia.info](#) CUMPLE con todos los puntos revisados en la misma. Pulse aquí.

Por tanto, en el plazo aproximado de 24 horas se podrá apreciar el cambio de estado del sello "QWEB certificada para BUSCADORES", que se muestra en dicha página web y certifica a los visitantes que cumple con todos los requerimientos de calidad de los principales buscadores, algo fundamental para lograr un buen posicionamiento en ellos. Ver / descargar.



Compartir

Me gusta

Regístrate para ver qué les gusta a tus amigos.

Twitter

0 comentarios Tags: qweb, webmaster

10 Sep 2011

## Importante aviso para webmasters ...

Escrito por: [José María Amador Vidal](#) el 10 Sep 2011 - [URL Permanente](#)

AVISO : no abrir ni urls intermedias, ni IPs de este mensaje, pues se tratan de zombiesbots.

IMPORTANTE PARA WEBMASTERS ...

OS RECOMENDAMOS BANEAR MEDIANTE htaccess y a través de la opción correspondiente en vuestro panel de control del administrador de contenidos, la siguiente IP : 95.163.66.184

El código a incluir en el archivo htaccess es:

```
Order Allow,Deny
Allow from All
Deny from 95.163.66.184
```

Os informamos que los varios intentos de intrusión a causa de scripts sospechosos por inyección de código malicioso han sido identificados por antivirus y tienen su origen en un servidor remoto de origen en la IP : 95.163.66.184

Se trata de una dirección situada en Moscú (Rusia), para ver geolocalización se puede utilizar el siguiente motor de rastreo. Pulse aquí.

Intentos de intrusión.

- 6 septiembre de 2011, 20:59
- 7 septiembre de 2011, 2:25
- 7 septiembre de 2011, 11:08
- 7 septiembre de 2011, 18:13
- 8 septiembre de 2011, 12:37

Estos han sido varios de los "logs" de intentos de intrusión

Tipo de ataque. Web Attack : Blackhole Toolkit Website 15  
 Riesgo. Alto  
 Equipo atacante. 95.163.66.184,80  
 Dirección de origen. 95.163.66.184

URLs atacantes.

Domínios intermedias entre las IPs origen y destino, es decir, utilizadas para la infección que coinciden con firmas de ataques conocidos.

- loveofyou.cu.cc
- jicabinetry.cu.cc
- overloved.cu.cc
- detectok.cu.cc
- 10fourmusic.cu.cc

Para más información en Symantec. Ver / descargar.

Observaciones : Se da la particularidad de que los dominios cu.cc no pertenecen a un país en concreto, y son gratuitos, de modo que se pueden constituir hasta 5 sitios web gratis a partir de la inscripción de un perfil de usuario en dicha plataforma, número que coincide con las 5 urls atacantes, y los 5 intentos de intrusión.

Compartir

Me gusta

Regístrate para ver qué les gusta a tus amigos.

Twitter

0 comentarios Tags: anti malware, networkers community, symantec, webmaster, htaccess

21 Ago 2011

## Traffic Rank & Toolbar ALEXA

Escrito por: [Carmen Martínez Ibáñez](#) el 21 Ago 2011 - [URL Permanente](#)

Perfil de usuario, rango de tráfico y barra de herramientas.

Alexa - Web Information Company, dispone de uno de los directorios de Internet más completos del mundo, ofrece una revisión diaria de su "Traffic Rank" y la posibilidad de disponer de su "Toolbar" personalizada al sitio en la red que más te convenga para su descarga por parte de los cibermatas que visitan con regularidad sus páginas electrónicas.



Con este fin se ha creado un perfil de usuario en esta comunidad de webmasters tras valorar el número de suscriptores que se han ido agregando y de quienes dimos referencia en nuestra última noticia publicada al respecto de los cambios en el análisis estadístico de nuestros sitios en internet.

Asimismo, se ha actualizado el rango de tráfico mediante una evaluación preliminar del dominio principal de nuestra batería de webs. Y finalmente, creamos una barra de herramientas en la que se contienen los enlaces e hipervínculos dinámicos que nos definen como generadores de contenidos. Ver / descargar.

Compartir

Me gusta

Regístrate para ver qué les gusta a tus amigos.

Twitter

0 comentarios Tags: networkers community, alexa, webmaster, toolbar

05 Ago 2011

## QWeb.es : Certificado de adecuación a buscadores

Escrito por: [Carmen Martínez Ibáñez](#) el 05 Ago 2011 - [URL Permanente](#)



Si ya hace unos meses os informamos de nuestro compromiso a través de CuWhois por cumplir la "Ley de Servicios de la Sociedad de Información y Comercio Electrónico" - LSSICE. Pulse aquí.

Ahora y ante las directrices de indexación en buscadores o los requerimientos por satisfacer los estándares de calidad en la red, hemos iniciado el proceso de certificación de estrategia.info por QWEB con el fin de alcanzar una oferta optimizada de códigos y contenidos en cumplimiento de las normas.

Ver/descargar - Certificado + Declaración.

Continuación ...

Compartir

Me gusta

Regístrate para ver qué les gusta a tus amigos.

Twitter

0 comentarios Tags: qweb, webmaster, lssi, tsicce, cuwhois

27 Jul 2011

## Glasnost : ISP Test

Escrito por: [Carmen Martínez Ibáñez](#) el 27 Jul 2011 - [URL Permanente](#)



Max Planck Institute for Software Systems con el fin de aportar transparencia a internet ha lanzado en la red : Glasnost ISP Test, un sistema de software que comprueba si ciertas de sus aplicaciones o la velocidad de procesamiento de su PC y el tráfico de red están bloqueados o estrangulados en la conexión de banda ancha suministrada por su ISP (Internet Service Provider), es decir, si se corresponde con la prevista por contrato con la configurada y compartida por su proveedor de servicios.

Características técnicas.

Los exámenes glasnost a demanda, son independientes uno de otro comprendiendo una duración total que puede oscilar alrededor de los 8 min. de espera antes de emitir su respuesta de información para cada prueba específica.



- P2P apps :**
1. BitTorrent.
  2. eMule.
  3. Gnutella.

- Standard apps :**
4. Email (POP).
  5. Email (MAF4).
  6. HTTP transfer.
  7. SSH transfer.
  8. Usenet (NNTP).

- Video-on-Demand :**
9. Flash video ...

Las pruebas consisten en la comparación de desempeños a diferentes flujos entre el host y los servidores dispuestos para su medición, le permiten detectar el tráfico en función del puerto de entrada o salida y la carga útil de los paquetes de datos entre sus procesos.

Continuación ...

Compartir

Me gusta

Regístrate para ver qué les gusta a tus amigos.

Twitter

0 comentarios Tags: max planck institute, isp, glasnost, mpi

25 Jul 2011

## Banear IPs con Simple PHP Blog

Escrito por: [José María Amador Vidal](#) el 25 Jul 2011 - [URL Permanente](#)

Este artículo es continuación de SPHP Blog : Método anti-spam. Tras crear una carpeta específica de spam en nuestra casilla de e-mail mediante la estrategia de crear un filtro (por ej. en función de la similitud y congruencia de los asuntos) de modo que se envíe la copia de los mensajes recibidos como comentarios en nuestra página web a una forma táctica hasta recuperar la estabilidad de la página web, y continuar con la verificación de los usuarios anónimos que nos están esparmeando con el fin de banearlos usando htaccess y acabar con el suceso. De la siguiente manera :

1. En el módulo scripts del blog, concretamente en el archivo sb\_functions.php añadir lo que a continuación se indica :

```
function getRealIP() {
if (tempy($ _SERVER[HTTP_CLIENT_IP])
return $ _SERVER[HTTP_CLIENT_IP];
if (tempy($ _SERVER[HTTP_X_FORWARDED_FOR])
return $ _SERVER[HTTP_X_FORWARDED_FOR];
return $ _SERVER[REMOTE_ADDR];
}
```

2. Insertar el siguiente fragmento en comment\_add\_cgi.php :

```
$ _SERVER[HTTP_CLIENT_IP], $ _SERVER[HTTP_X_FORWARDED_FOR], $ _SERVER[REMOTE_ADDR];
$_SERVER[REMOTE_ADDR], stripslashes($ _POST[ comment_url ]), stripslashes($ _POST[ blog_text ] )
);
```

3. Así obtendremos las IPs de los spammers en origen porque estas codificaciones permiten averiguarlas de forma remota haciéndolas constar entre los datos que hay en los correos electrónicos recibidos como copias de seguridad del mensaje enviado al servidor a través del formulario de comentarios en el blog y rellenado por el spammer. Este sistema opera sustituyendo el nombre y web del remitente por su IP, conservando el resto del mensaje, e-mail y comentario.

- a) Ahora ya podremos hallar su procedencia a partir de las direcciones IP que han sido identificadas con el sistema descrito, y mediante el uso de [whatsmyipaddress.com/Ip](#)
- b) También es posible comprobar si se trata de botnets, colocando la IP en la casilla correspondiente de [rbltest.com](#)
- c) O bien, averiguar si se encuentran en listas negras de spam, con [whatsmyipaddress.com/blacklist-check](#)

4. Tras esta evaluación preliminar, seleccionaremos las IPs candidatas a banear y generaremos el código para insertar en el archivo htaccess del blog según el ejemplo ofrecido por todos [dynamicdrive.com/userban](#)

Si durante el proceso de indagación os colapsan el servidor por el envío masivo, podéis interrumpir el servicio de comentarios de una forma táctica hasta recuperar la estabilidad de la página web, y continuar con la investigación devolviendo a su estado original la carpeta de la que os indicamos como debéis cambiar los permisos para que no se graben en el servidor los mensajes spammers, y posteriormente los sigais recibiendo para conseguir averiguar las IPs a banear.

Para ejemplificar, en el blog y atendiendo al menú de configuración tras acceder con el username y password en el sistema de administración de contenidos, debéis primero deshabilitar el envío de comentarios en el blog. Posteriormente tras la incidencia, habilitáis de nuevo la opción de configuración para agregar comentarios.

Por otro lado, en cambio, y siguiendo con el ejemplo, si en el servidor FTP el lugar donde se reciben los mensajes masivos está contenido en el módulo "contenits", carpeta "06" y subcarpetas "10", en su interior se halla la otra carpeta "coments" y en su interior se halla la carpeta específica, y su ruta dependerá de la fecha del post. De esta forma, si el ejemplo que hemos puesto, es del mes de octubre del año 2010, tendremos que abrir nuestro FTP (File Transfer Protocol) y en el módulo "contenits" del blog, encontraremos en la carpeta "06" y subcarpetas "10", los "coments" acumulados de horas, días o semanas, etc... pudiendo borrarlos por completo en una sola acción.

En definitiva, en el fichero adjunto, ofrecemos IPs a banear que convierten nuestro archivo htaccess en el que consta a continuación y con el que podéis guiarnos para saber incluir la codificación de todos los datos. Pulse aquí.

Nota : Todos los documentos adjuntos de este artículo están en formato doc porque solamente son para visualizar su contenido que es el que encontrareis utilizando un bloc de notas para leer o modificar tanto los archivos sb\_functions.php y comment\_add\_cgi.php, como htaccess.

Compartir

Me gusta

Regístrate para ver qué les gusta a tus amigos.

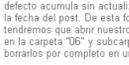
Twitter

0 comentarios Tags: networkers community, sphpblog, webmaster, ip, spammer, gnu, pineapp, unjippe, htaccess

22 Jul 2011

## SPHP Blog : Método anti-spam

Escrito por: [José María Amador Vidal](#) el 22 Jul 2011 - [URL Permanente](#)



Qué podemos hacer los bloggers cuando no disponemos de sistemas de seguridad para impedir avalanchas de comentarios que provienen de usuarios anónimos buscando insertar links enteros a través de sistemas automatizados en la red para aumentar su posicionamiento en Google u otros buscadores.

Ante esta situación hemos de ser reflexivos, sensatos y obrar con total serenidad. Todos los webmasters sabemos que no será ni la primera ni la última vez que esto ocurra. Por tanto, lo más coherente es idear un sistema para contrarrestar posibles incidencias futuras no solamente la presente.

De este modo, primero hay que aclarar que este tipo de situaciones se producen en parte a causa de los algoritmos que utilizan los motores de búsqueda en Internet para calibrar la importancia de un sitio. Por esta razón, muchos cibermatas se empeñan a toda costa en utilizar métodos poco aconsejados como es la implementación de máquinas que trabajen de manera automática las 24 horas, enviando textos con vínculos a su sitio mediante un mayor número posible de enlaces a sus webs desde todas las partes de mundo con el fin de conseguir aumentar su posición y las posibilidades de promoción de sus productos.

Este artículo se refiere a los webmasters que usan Simple PHP Blog porque ante esta estrategia de marketing online sin escrúpulos o principios éticos, son los que sufren mayores problemas por su causa. Este sistema de bitácoras fue ideado con código abierto, es decir, disponible como freeware, y cumple bien con su función de publicar y gestionar contenidos, muy común en la mayoría de bitácoras disponibles, sin embargo, su "capcha" anti-spam no detiene a los "droids", explicaremos esto.

Por ejemplo, si nos fijamos en un prototipo como el que encontramos habitualmente. Pulse aquí. Vemos que en el oficio de calceamiento se encuentra el formulario para agregar comentarios, en el que se rellenan datos que luego y posteriormente son enviados al servidor de la página electrónica tras introducir el valor numérico y marcar "publicar comentario".

En su origen se entendían en blogs "forms", pero esto se ha demostrado últimamente como inútil, pues durante el día 22 de julio del 2011, desde las 00 : 05 h. hasta 22 : 35 h. hemos recibido un mensaje cada 5-10 min. aproximadamente que es el periodo en el que se han programado.

Como podemos ver, que de esta forma, ya que Simple PHP Blog, no dispone de otra operativa anti-spam y tampoco tiene posibilidad de moderación de comentarios como muchos CMS (Content Management System) para evitar su publicación.

El método anti-spam que hemos ideado y que recomendamos poner en práctica, es el siguiente :

1. Si nos fijamos en el botón de "Publicar comentario", este está enlazado al archivo "comment\_add\_cgi.php", cuyo código es el que activa el postado de contenidos, a través de sentencias y rutinas.
2. El código fuente para php, está disponible en el siguiente enlace. Pulse aquí. Si nos fijamos tras abrir con el bloc de notas el fichero, encontraremos el fragmento de descripción que a continuación se indica.

```
$ok = write_comment($ _POST[ 'y' ], $ _POST[ 'm' ], $ _POST[ 'entry' ] ...
$ok = write_comment($ _POST[ 'y' ], $ _POST[ 'm' ], $ _POST[ " ] ...
```

4. Con esta maniobra conseguiremos recibir por correo electrónico el comentario publicado (si así lo hemos indicado en la opción del menú de configuración del blog), pero en cambio no se posteará en nuestra página web, como si estuviera moderado en espera, pudiendo distinguir el spam de los comentarios interesantes mediante una sencilla visualización de los e-mails.

5. A donde van a parar los mensajes, es la cuestión más importante, el sistema Simple PHP Blog, por defecto acumula sin actualizar o publicar los comentarios en una carpeta específica, y su ruta dependerá de la fecha del post. De esta forma, si el ejemplo que hemos puesto, es del mes de octubre del año 2010, tendremos que abrir nuestro FTP (File Transfer Protocol) y en el módulo "contenits" del blog, encontraremos en la carpeta "06" y subcarpetas "10", los "coments" acumulados de horas, días o semanas, etc... pudiendo borrarlos por completo en una sola acción.

6. El webmaster al acceder al sistema de administración tras introducir la clave de acceso (username y password) observará junto al mensaje de bienvenida el número de comentarios que se han intentado postear y que recomendamos no actualizar antes de borrarlos en el servidor FTP.

Finalmente, con este método anti-spam, evitamos la emisión de miles de mensajes no deseados, y disponemos de los que nos interesen en nuestra casilla de e-mail que podemos publicar a voluntad si son imprescindibles para nuestros lectores.

Continuación ...

Compartir

Me gusta

Regístrate para ver qué les gusta a tus amigos.

Twitter

0 comentarios Tags: networkers community, sphpblog, webmaster, spammer, osi, akismet

Leer siguientes » [« Leer anteriores](#)

## Networkers

Webmasters

21 Jul 2011

### Speed Test Mini

Escrito por: [Carmen Martínez Ibañez](#) el 21 Jul 2011 - [URL Permanente](#)



Fuente : [Speed Test](#).

Puede ser host de una prueba de velocidad gratuita en su propio servidor con la misma tecnología que Speedtest.net. La configuración es extremadamente simple y el único requisito es que su servidor web admita PHP, ASP.NET o ASP.

Esta aplicación se ofrece en sus condiciones actuales, de forma gratuita y sin soporte: debe usarla bajo su responsabilidad. Incorporaremos funciones nuevas cada varios meses mediante actualizaciones obligatorias. Por ello, deberá descargarla nuevamente cada cierto tiempo.

Si bien Speedtest.net Mini funciona en casi cualquier servidor web, algunos de ellos requieren un ligero ajuste en la configuración. Lea el archivo de resolución de problemas que se incluye en mini.zip para conocer más detalles.

Si necesita una prueba de velocidad permanente con informes detallados o con su propia marca, consulte el sitio web de Ookla.com

Instrucciones de configuración.

- 1.Descargue mini.zip.
- 2.Descomprímalo en su servidor.
- 3.Defina si será PHP, ASP.NET o ASP.
- 4.Seleccione qué archivo de indexación desea usar.
- 5.Cambie el nombre del archivo por index.html.
- 6.Cargue index.html en su navegador.

También puede copiar el código comentado desde index.html y pegarlo en una página web existente. Asegúrese de mantener la carpeta "speedtest" y el archivo "speedtest.swf" en el lugar correspondiente.

[Descargar ahora / Ver demo.](#)

Compartir

Me gusta Regístrate para ver qué les gusta a tus amigos.

Twitter 0

0 comentarios Tags: speedtest net, networkers community, ip, webmaster

18 Jul 2011

### Libro electrónico en Biblioteca Universitaria

Escrito por: [Carmen Martínez Ibañez](#) el 18 Jul 2011 - [URL Permanente](#)



La reciente incorporación entre los documentos contenidos en los lectores de libros electrónicos de la Biblioteca de la Univ. de las Palmas de Gran Canaria de "Internet eley Seguridad", una metodología de aplicación para combatir malware que proviene de un servidor remoto de origen desconocido e inyecta código malicioso en sitios legítimos, que presentamos en formato de comunicación técnica en las 7 BYMC - Jornadas de Blogs y Medios de Comunicación (15-16 abril 2010), cuyo evento, se celebró en la sede de la Asoc. de Prensa y con la colaboración de la Univ. de Granada (España). [Pulse aquí.](#)

Compartir

Me gusta Regístrate para ver qué les gusta a tus amigos.

Twitter 0

0 comentarios Tags: networkers community, anti malware, e book, bymc, webmaster

08 Jul 2011

### Trend Micro : HouseCall + Smart Protection Network

Escrito por: [José María Aménos Vidal](#) el 08 Jul 2011 - [URL Permanente](#)



Si no se ha quedado Ud. tranquilo cuando después de realizar una descarga que parecía del todo segura, aparece con la aplicación que descargó un aviso de riesgo de infección que su anti-virus le notifica que ha bloqueado, está procesando, o ha puesto en cuarentena. El programa de rastreo que le proponemos es la solución a su intranquilidad después del suceso.

Es rápido, sencillo y seguro, no es necesario instalar en el ordenador y ofrece garantías de detectar las infecciones que le preocupan. Se trata de HouseCall, un explorador en línea antivirus y antispyware gratuito muy conocido y eficaz de Trend Micro disponible bajo petición que identifica y elimina virus, troyanos, complementos del explorador no deseados, etc ...

Una exploración rápida de áreas cruciales del sistema y de malware activo que hace uso de Smart Protection Network para garantizar la detección y solución a las amenazas más

recientes independientemente del estado de protección y seguridad existente en su PC. Añade compatibilidad con versiones de 32 bits para Windows XP, y 64 bits de Windows 7 y Vista. [Pulse aquí.](#)

Compartir

Me gusta Regístrate para ver qué les gusta a tus amigos.

Twitter 0

0 comentarios Tags: trend micro, anti malware, anti spyware, windows

08 Jun 2011

### Symantec : Análisis automatizado de sitios web

Escrito por: [José María Aménos Vidal](#) el 08 Jun 2011 - [URL Permanente](#)



Evaluación : SEGURO.

La evaluación de Norton Safe Web es un resultado del sistema de análisis automatizado de Symantec realizado a estrategia.info en un estado de problemas de seguridad y no encontró ninguno en nuestro sitio web ubicado en Italia. [Pulse aquí.](#)

Información general.

Resumen

- Amenazas para el equipo: 0
- Amenazas para la identidad: 0

- Factores de molestia: 0

Total de amenazas encontradas : 0

Informe.

- Virus : 0
- Descargas no autorizadas : 0
- Descargas maliciosas : 0
- Gusanos : 0
- Aplicaciones sospechosas : 0
- Cambios sospechosos en el navegador : 0
- Riesgos para la seguridad : 0
- Virus heurísticos : 0
- Publicidad no deseada : 0
- Troyanos : 0
- Ataques de phishing : 0
- Spyware : 0
- Puertas traseras : 0
- Software de acceso remoto : 0
- Ladrones de información : 0
- Marcadores : 0
- Programas de descarga : 0
- Vínculo integrado hacia un sitio malicioso : 0



Compartir

Me gusta Regístrate para ver qué les gusta a tus amigos.

Twitter 0

0 comentarios Tags: anti malware, networkers community, anti spyware, symantec, norton, webmaster

30 May 2011

### Web CEO desktop & online

Escrito por: [Carmen Martínez Ibañez](#) el 30 May 2011 - [URL Permanente](#)

Fuente : [Web CEO](#).

Os mencionamos este programa por las prestaciones que ofrecen tanto la versión "desktop" como "online". [Pulse aquí.](#)

## web ceo online

En principio, nuestra primera intención al utilizar una herramienta de estas características estaba enfocada a la monitorización del alojamiento FTP - File Transfer Protocol de nuestro sitio en internet. Por ejemplo, en la opción para descargar en nuestro PC tras parametrizar los campos y configurar el análisis por monitoreo, recibimos un informe por correo electrónico que nos indica que tal se está desarrollando el servidor de nuestro espacio web durante la última semana, en el caso de estrategia.info, se ofrece una muy buena valoración general y puntuación de ejecución igual a 7. [Pulse aquí.](#)

No obstante, y la gran utilidad de disponer en nuestro ordenador de un sistema que nos permita controlar el rendimiento de nuestros servidores en la red, en realidad, hay otros programas que nos ofrecen un modo más detallado para cumplir con dicha función, por mencionar alguno [APlus Monitoring & PingPro](#).

Por esta razón, la aplicación informática de Web CEO está específicamente dirigida a SEO - Search Engine Optimization, backlinks discovery, etc ... para webmasters que buscan un modo de mejorar su posicionamiento en Internet, la promoción en motores de búsqueda, la difusión de palabras clave, la selección de enlaces, y muchas otras herramientas de optimización web.

Entre otros ejemplos, dispone de sistemas que nos permitirán incluso medir el tráfico en nuestros dominios y subdominios, pero en este último aspecto, también existen aplicaciones más específicas como serían el caso de los programas [Web Analytics](#).

Sin embargo, tanto la versión descargable como en línea ofrecen servicios gratuitos y avanzados que se complementan, es por todo ello, que os recomendamos ambas versiones.

Compartir

Me gusta Regístrate para ver qué les gusta a tus amigos.

Twitter 0

0 comentarios Tags: networkers community, web ceo, aplus monitoring, seo, webmaster, pingpro, pivik

29 May 2011

### APlus Monitoring & PingPro

Escrito por: [Carmen Martínez Ibañez](#) el 29 May 2011 - [URL Permanente](#)

APlus Monitoring se ha convertido actualmente en PingPro, empresa especializada en la monitorización de servidores de Booro Group.

Esta prestación para nuestras páginas web empieza a ser una utilidad para el webmaster cada vez más necesaria y este servicio viene a cumplir con esta función. Si su sitio en internet está fuera de línea tan sólo un 1 % del tiempo total de verificación, esto se traduce en más de 6 horas al mes.

El monitoreo del sitio se convierte así en una herramienta indispensable para recibir alertas en el momento en que su página web no se encuentra en red por causas que normalmente escapan a su control.

Con PingPro sólo tiene que añadir sus datos y recibirá avisos o notificaciones de inmediato por correo electrónico, mensajería de texto SMS y RSS, es decir, tan pronto como hay un problema, dándole la oportunidad de prevenir posibles incidencias técnicas e incluso resolverlas teniendo aquella información necesaria que le permitirá tomar las medidas adecuadas.

Recibirá informes periódicos de seguimiento en cuanto a disponibilidad y rendimiento, errores en línea o tiempo de inactividad proporcionando los datos que le permitirán un correcto y preciso mantenimiento de su página electrónica con el fin de conseguir un funcionamiento sin problemas.

Sin estos reportes detallados no puede conocer de las interrupciones en la red, ni tampoco la causa de las mismas. En cambio, monitorizar su servidor desde varias ubicaciones en todo el mundo supervisará su sitio web.

Los controles de detección se llevan a cabo en intervalos de minutos y existe la opción de controlar hasta tres servidores de acceso de forma totalmente gratuita. [Pulse aquí.](#)

Compartir

Me gusta Regístrate para ver qué les gusta a tus amigos.

Twitter 0

0 comentarios Tags: booro group, aplus monitoring, pingpro, webmaster

28 May 2011

### Site Speed Lab

Escrito por: [José María Aménos Vidal](#) el 28 May 2011 - [URL Permanente](#)

Entre las herramientas para la monitorización del rendimiento de una dirección electrónica, destacamos la desarrollada por Site Speed Lab, un laboratorio para el análisis de velocidad de los sitios web.

Por su utilidad en cuanto a : Website latency + DNS lookup + Page speed, os lo recomendamos. Por ejemplo, para estrategia.info los resultados son los siguientes tras la aplicación de los tests.

a) **Website Latency** (latencia del sitio web).

La latencia afecta la tasa de intercambio de paquetes de datos en la red entre el ordenador del usuario y el servidor.

Según el Ping Test Graph, la latencia media es de 96 ms. Esta prueba se realizó a partir de 5 lugares diferentes : 1) New York, 2) Tampa, Florida. 3) Frankfurt, Germany. 4) Montreal, Canada. 5) Gloucester, United kingdom. La nota media es buena (94 % sitios web son más lentos). [Pulse aquí.](#)

b) **DNS Lookup** (búsqueda del DNS - Domain Name System).

La obtención de la dirección IP del servidor (61.92.42.79) antes de descargar la página web, es decir, el factor de resolución DNS. Test desde los 5 puntos mencionados, arroja un tiempo medio de recepción de IP de 0.16 s (que es mejor que el 62 % de todos los sitios). [Pulse aquí.](#)

c) **Page Speed** (velocidad de la página).

La velocidad de descarga de las páginas electrónicas depende de muchos factores. Los principales son el ancho de banda, el número de descargas simultáneas, la distancia entre el usuario y el servidor del dominio, etc ...

Mediciones recientes por Page Speed Test han demostrado que los sitios de descarga es de 79.430 Kb/s (que es mejor que el 58 % de todos los sitios de su región). [Pulse aquí.](#)

De este modo, según la fórmula propuesta y el diagnóstico detallado que se basa en datos del 27 de mayo del 2011 (desde primeros de julio del 2010 se han llevado a cabo 67 pruebas desde las ubicaciones señaladas con el fin de evaluar la página principal), las pruebas realizadas sobre Website Latency (94 %) + DNS Lookup (62 %) + Page Speed (58 %) nos indican por término medio un Site Speed Test del 71 %.

Compartir

Me gusta Regístrate para ver qué les gusta a tus amigos.

Twitter 0

0 comentarios Tags: site speed lab, ip, webmaster

### Check Safe Website

Escrito por: [José María Aménos Vidal](#) el 28 May 2011 - [URL Permanente](#)

Fuente : [RadaBG](#).

Tras un largo recorrido desde el 25 de junio al 3 de septiembre del 2009 en el que implementamos las medidas de seguridad según la metodología que creamos con este propósito para ofrecer orientaciones a webmasters con el fin de combatir malware que proviene de un servidor remoto de origen desconocido y que inyecta código malicioso en sitios legítimos, que presentamos en una comunicación técnica en la modalidad de flash talks en las VII Jornadas de Blogs y Medios de Comunicación - BYMC 7 (15-16 abril 2010) desarrolladas en la sede de la Asociación de Prensa y con la colaboración de la Universidad Granada, y que también tuvo difusión en la [agencia interactiva](#) y de [aplicaciones web](#) - PulpolaB (Barcelona, España), por su probada eficiencia.

Os comunicamos que RadaBG utilizado por algunas de las empresas más famosas del mundo y por miles de importantes bloggers, que comprueba la seguridad de dominios y subdominios en Internet a través de su funcionalidad con sitemaps, y que es especialmente útil para los espacios con contenido generado por usuarios (UGC - User Generated Content), nos ha auditado mediante su herramienta Smart Analytics300 y certifica el nivel de seguridad de estrategia.info como sitio con navegación segura y fiable.

Compartir

Me gusta Regístrate para ver qué les gusta a tus amigos.

Twitter 0

0 comentarios Tags: anti malware, networkers community, radabg, pulpolab, bymc, webmaster

24 May 2011

### Módulo EvenNews para XOOPS

Escrito por: [Carmen Martínez Ibañez](#) el 24 May 2011 - [URL Permanente](#)

Fuente : [Xoops](#).



EvenNews es un módulo de CMS para XOOPS en código abierto OSI y con licencia importante bloggers, que comprueba la seguridad de dominios y subdominios en Internet a través de su funcionalidad con sitemaps, y que es especialmente útil para los espacios con contenido generado por usuarios (UGC - User Generated Content), nos ha auditado mediante su herramienta Smart Analytics300 y certifica el nivel de seguridad de estrategia.info como sitio con navegación segura y fiable.

La instalación es la habitual para este tipo de plataformas enfocadas a la creación de comunidades en línea.

- 1) Descargue el archivo en formato comprimido y extraiga su contenido.
- 2) Cargue vía FTP la carpeta con el nombre "evennews" en la subcarpeta de módulos de su servidor.

3) Acceda a su área de administración en el CMS y en la opción de módulos active y configure "evennews". Recomendamos la utilización de las pruebas de envío o recepción de boletines electrónicos antes de la entrega definitiva de los mensajes a su lista de correo o libreta de direcciones, sus prestaciones para fuentes en HTML lo hacen una herramienta necesaria para sus presentaciones y comunicaciones.

Compartir

Me gusta Regístrate para ver qué les gusta a tus amigos.

Twitter 0

0 comentarios Tags: webmaster, xoops, osi, gnu

15 May 2011

### Free Software Foundation apoya Web M

Escrito por: [Carmen Martínez Ibañez](#) el 15 May 2011 - [URL Permanente](#)

Fuente : [Globleia](#).

Una de las piezas fundamentales para la adopción de HTML5 es algún estándar contenido en video y en ello hay debate entre los pesos pesados de Internet. Por una parte está un grupo que entre sus filios se encuentra Apple y Microsoft, quienes apoyan el códec H.264 el cual si bien tiene muy buen rendimiento, es cerrado y está rodeado de patentes, en cambio en la otra esquina, liderados por Google, están quienes buscan la adopción del estándar Web M el cual usa el códec libre VP8.



Google para dar el ejemplo, en próximas versiones de Chrome dejará de dar soporte al formato H.264 pasando solo al soporte de Web M al igual al igual a Firefox y Safari, y en este apoyo ahora se suma la Free Software Foundation (FSF) en donde además dejan en clara su posición contraria al uso del códec H.264.

Es cuestión de tiempo para llegar a consenso y tener las bases definitivas de lo que será el futuro de Internet bajo HTML5.



Compartir

Me gusta Regístrate para ver qué les gusta a tus amigos.

Twitter 0

0 comentarios Tags: mozilla firefox, globleia, google, safari, microsoft, apple, fsf

[Leer siguientes](#) [Leer anteriores](#)

## Networkers

Webmasters

14 May 2011

### Web Analytics

Escrito por: [José María Amenós Vidal](#) el 14 May 2011 - [URL Permanente](#)

De entre muy variadas opciones gratuitas para monitorizar nuestros sitios en Internet, encontraremos una diversa gama de posibilidades, entre las que podemos destacar [Woopra](#) y [GoingUp](#).

Sin embargo, la que hemos instalado en [estrategia.info](#) para análisis web, es la de [Piwik](#) que consideramos es la mejor aplicación de este género, por tratarse de freesoftware en código abierto (OSI - Open Source Initiative), que se carga en el servidor FTP y dispone de una base de datos MySQL. [Pulse aquí](#).



Está disponible en múltiples idiomas y mide en tiempo real todo el tráfico de la red relativo al dominio específico, con informes detallados sobre usuarios, motores de búsqueda, palabras clave, y otras muchas prestaciones. Encontrarás información relacionada a través, aplicaciones para móviles y todos los requerimientos para su instalación. [Pulse aquí](#).

Para más información: "The Top 8 Killer Alternatives to Google Analytics" de Jarel Remick en [Appstom Web](#) a 30 de diciembre del 2010, traducido al castellano por [Ideas Web](#) y publicado el 3 de enero del 2011.

Compartir

[Me gusta](#) [Regístrate para ver qué les gusta a tus amigos.](#)

[Twitter](#) (0)

[0 comentarios](#)

Tags: [networkers community](#), [woopra](#), [goingup](#), [piwik](#), [webmaster](#), [seo](#), [osi](#)

08 May 2011

### Test MobiReady + MobileOK Checker

Escrito por: [José María Amenós Vidal](#) el 08 May 2011 - [URL Permanente](#)

MobiReady.

La herramienta de prueba [MobiReady](#) evalúa el grado de calidad de visualización de una página web a través de cualquier dispositivo móvil con objeto de servir a los webmasters y saber así el nivel de adaptación de sus webs con el fin de ser mostradas en teléfonos con conexión a Internet.

Ejemplo: [Test MobiReady](#). [Pulse aquí](#).

Un análisis a fondo de las páginas electrónicas, utilizando las mejores prácticas o estándares y que proporciona un informe completo expresado en una puntuación de 1 a 5 que determina qué tan bien se desenvuelve el sitio en los dispositivos móviles.

MobileOK.

[MobileOK Checker](#) de W3C (World Wide Web Consortium) forma parte de [MobiWeb 2.0](#) proyecto apoyado por la Unión Europea en el séptimo Programa Marco de Investigación (European Union's 7th Research Framework Programme - FP7) basado en código abierto (OSI - Open Source Initiative) y que chequea el estado de preparación de un espacio web para ser visualizado por teléfono móvil.

Ejemplo: [MobileOK Checker](#). [Pulse aquí](#).

Compartir

[Me gusta](#) [Regístrate para ver qué les gusta a tus amigos.](#)

[Twitter](#) (0)

[0 comentarios](#)

Tags: [ready mobi](#), [webmaster](#), [osi](#), [w3c](#)

09 Abr 2011

### Internet via telefonía móvil e iPad

Escrito por: [José María Amenós Vidal](#) el 09 Abr 2011 - [URL Permanente](#)

Las informaciones a través de nuestras ediciones y medios electrónicos o digitales son accesibles a través de la red de telefonía inalámbrica.

En la era de las comunicaciones por vía satélite, nuestro espacio en internet de Word Press nos permite mostrar las noticias en tiempo real para iPad y telefonía móvil. [Pulse aquí](#).

Compartir

[Me gusta](#) [Regístrate para ver qué les gusta a tus amigos.](#)

[Twitter](#) (0)

[0 comentarios](#)

Tags: [word press](#), [webmaster](#)

### Premios de Internet

Escrito por: [Carmen Martínez Ibáñez](#) el 09 Abr 2011 - [URL Permanente](#)



Hemos inscrito a Edimed - Ediciones y medios electrónicos o digitales u otros medios en candidatura única con el fin de optar a su selección en la categoría de sitio web: Mejor Comunicador.

El mismo enlace de votación ha sido incluido en los sitios dependientes de [estrategia.info](#) para pedirnos vuestro voto. [Pulse aquí](#).

Compartir

[Me gusta](#) [Regístrate para ver qué les gusta a tus amigos.](#)

[Twitter](#) (0)

[0 comentarios](#)

Tags: [networkers community](#), [premios de internet](#), [webmaster](#)

07 Mar 2011

### LSSI - Ley de Servicios de la Información

Escrito por: [Carmen Martínez Ibáñez](#) el 07 Mar 2011 - [URL Permanente](#)

Si eres webmaster estás obligado a cumplir la llamada "Ley de Servicios de la Sociedad de Información y Comercio Electrónico". Tanto si mantienes un blog, web personal, comercial, etc ...

Las multas por incumplir la LSSI pueden ser de varios miles de euros. Más información en [Lssi.es](#). Para evitar posibles problemas es mejor que la cumplas de modo que no puedan denunciarte y además darás más confianza a tus visitas.

Si resides en España y tienes una web cumple la ley que regula la legalidad de los espacios web en Internet según la legislación española, y por la cual hemos validado nuestro dominio [estrategia.info](#) para que cumpla la LSSI - LSSICE Ley de Servicios de la Información. [Pulse aquí](#).

- Datos del propietario de la web.
- Terminos y condiciones.
- Uso de la web.

(\*) La información se encuentra almacenada en los servidores de [cuwhois](#), y los datos encriptados mediante algoritmo.

Compartir

[Me gusta](#) [Regístrate para ver qué les gusta a tus amigos.](#)

[Twitter](#) (0)

[0 comentarios](#)

Tags: [webmaster](#), [lssi](#), [lssice](#), [cuwhois](#)

06 Mar 2011

### Truco para evitar problemas de reproducción a causa de un script

Escrito por: [José María Amenós Vidal](#) el 06 Mar 2011 - [URL Permanente](#)

En la experiencia de combinar en una página de Internet varios archivos con extensión [swf](#) en ocasiones se producen interferencias entre ellos, provocando un bucle infinito que impide la reproducción de alguno de los ficheros, apareciendo un mensaje de error que indica que un script de la página ralentiza su visualización provocando un fallo que bloquea la ventana del explorador.

Ante esta situación, independientemente de que hayamos verificado el buen funcionamiento de Java, actualizado Adobe Flash + Shockwave Player, y tengamos los complementos o plugins del navegador habilitados para ambos recursos, el problema por redundancia cíclica persiste por defecto en el ancho de banda, el rendimiento del ordenador y/o causa del navegador.

Por esta razón, la única opción que la queda al webmaster para normalizar el buen funcionamiento de la reproducción y evitarles problemas a los usuarios limitados por su ADSL o PC, es que se aplique una estrategia que permita abrir los diferentes archivos por orden consecutivo y no de forma simultánea.

Observamos que para los navegadores de Google, Safari, Opera, Netscape, Mozilla, Maxthon, etc ... entre los más utilizados normalmente no se producen este tipo bucles. Sin embargo, si se producen por redundancia **problemas con Internet Explorer 8**, porque suele ocurrir que si no introducimos el código fuente html adecuado que permita la apertura de los ficheros ordenadamente acabarán por interferirse entre ellos provocando que se bloqueen.

Por esta razón, tuvimos que idear un modo por el que el fichero inferior se abiera con posterioridad dejando tiempo suficiente para que se cargara el superior, y así ambos se reprodujeran sucesivamente sin que se colapsaran entre ellos.

De este modo, lo único que hemos hecho es introducir arriba un embed con el archivo de extensión [swf](#) para que se abra y reproduzca inmediatamente al abrir la página, y abajo hemos colocado un iframe que enlaza a un fichero con una etiqueta meta que permite un retardo de varios segundos o tiempo suficiente hasta que acto seguido conecte con el archivo que contiene el script que comanda la siguiente reproducción.

Así pues, para que no se produzca un bucle infinito que provoque por redundancia cíclica el mensaje de error que nos informa de que un script está provocando un problema de reproducción, hemos necesitado para el caso mencionado.

a) embed superior. Se colocará aquí el código embed del que depende la primera reproducción. También podría tratarse de un object.

b) iframe inferior. A continuación, el marco. Por ejemplo:

```
< iframe align="center" height="272" width="480" src="http://estrategia.info/fpc/descargas/gadget.htm"
frameborder="0" scrolling="no">
```

Y hemos colocado en el **gadget** el siguiente comando.

c) meta enlace. Este es el truco de la etiqueta.

```
< meta http-equiv="refresh" content="10; URL=http://estrategia.info/fpc/descargas/global.htm" />
```

El valor numérico igual a **10** se puede aumentar o disminuir según los segundos de retardo que se necesiten para redirigir el tráfico de modo que no se produzcan interferencias con el archivo **global** que contiene el script de la segunda reproducción.

Compartir

[Me gusta](#) [Regístrate para ver qué les gusta a tus amigos.](#)

[Twitter](#) (0)

[0 comentarios](#)

Tags: [mozilla firefox](#), [internet explorer](#), [maxthon](#), [google](#), [safari](#), [opera](#), [avart](#), [windows](#), [netscape](#), [microsoft](#), [webmaster](#), [adobe](#), [java](#), [gps](#)

04 Feb 2011

### Microsoft Translator

Escrito por: [José María Amenós Vidal](#) el 04 Feb 2011 - [URL Permanente](#)

Fuente: **Microsoft**.

El widget de la página web de Microsoft Translator te permite incorporar traducciones en tiempo real e in situ a tu sitio web. Prueba las nuevas características colaborativas que combinan la tecnología de la traducción automática con toda la capacidad de tu comunidad. [Pulse aquí](#).

Usuarios.

Los usuarios pueden ver las páginas en su propio idioma, sin tener que ir a un sitio web de traducción separado, y así compartirlas con amigos en sus varios idiomas. Puedes aprender más sobre cómo usar este widget, obtener ayuda o interactuar con otros propietarios de sitios Web en Microsoft Translator. [Pulse aquí](#).

Webmasters.

La Web crece a un ritmo veloz, con nuevos contenidos a cada segundo. La gama de usuarios de Internet presenta una diversidad lingüística cada vez mayor. Microsoft Translator está al frente de la innovación en la experiencia de la traducción web ayudando a los propietarios del contenido a atraer visitantes de todo el mundo a sus sitios. [Pulse aquí](#).

Ejemplo.

Traducir esta página con tecnología de Microsoft Translator

Continuación ...

Compartir

[Me gusta](#) [Regístrate para ver qué les gusta a tus amigos.](#)

[Twitter](#) (0)

[0 comentarios](#)

Tags: [microsoft](#), [webmaster](#)

23 Dic 2010

### PulpoLab : Cómo proteger de software malicioso la web

Escrito por: [Carmen Martínez Ibáñez](#) el 23 Dic 2010 - [URL Permanente](#)

Fuente: **PulpoLab**.

[PulpoLab](#) es una agencia interactiva de factura catalana en Barcelona (España) con más de una década de experiencia digital en la creación, diseño, maquetación y programación de aplicaciones web multimedia, para móvil y publicidad interactiva.

En su boletín de noticias del 13 de diciembre del 2009, hace un intensivo repaso de la metodología que utilizamos del 25 de junio al 3 septiembre del 2009, para hacer frente a los 14 ataques sufridos en [estrategia.info](#) a consecuencia de malware procedente de un servidor remoto de origen desconocido y que inyectaba código malicioso en nuestros sitios legítimos. [Pulse aquí](#).

Compartir

[Me gusta](#) [Regístrate para ver qué les gusta a tus amigos.](#)

[Twitter](#) (0)

[0 comentarios](#)

Tags: [anti malware](#), [networkers community](#), [pulpolab](#), [webmaster](#)

02 Dic 2010

### Rutina de comprobación y activación de cuenta

Escrito por: [José María Amenós Vidal](#) el 02 Dic 2010 - [URL Permanente](#)

En el desarrollo de la labor de webmaster al gestionar una comunidad virtual (por ej. con XOOPS), nos enfrentamos a menudo con solicitudes de activación de cuenta tras el registro de un usuario. En nuestros años de experiencia hemos llegado a la siguiente conclusión:

Si conocemos los e-mails.

1) La rutina de comprobación por cuestiones de seguridad nos obliga a confirmar que el dominio del correo electrónico del perfil a activar no se encuentre en la lista negra de sitios potencialmente peligrosos. Para ello, es conveniente utilizar la metodología [Google Safe Browsing + Malware Domain List](#), o si bien, [Norton Safe Web + McAfee Site Advisor](#).

2) El siguiente paso es insertar en el buscador de [Stop Forum Spam](#) el e-mail completo de solicitud para realizar una prospección de su historial en la red.

En caso de averiguar las IPs.

3) Podemos hacer comprobaciones adicionales de IP - Internet Protocol, para minimizar los riesgos que comportarían las activaciones de estas cuentas, o bien a través de [Zombie Detection System + Spamhaus](#). En resumen, estos tres sencillos pasos son requisitos esenciales y la base de una actuación correcta del administrador ante un desconocido que desea ingresar a nuestro sitio y con el fin de garantizar la normal actividad de la web.

Compartir

[Me gusta](#) [Regístrate para ver qué les gusta a tus amigos.](#)

[Twitter](#) (0)

[0 comentarios](#)

Tags: [networkers community](#), [stop forum spam](#), [anti malware](#), [malware domain list](#), [pineapp](#), [spamhaus](#), [ip](#), [google](#), [webmaster](#), [norton](#), [mcafee](#), [xoops](#), [gps](#)

11 Nov 2010

### ¿ Problemas con Internet Explorer 8 ?

Escrito por: [José María Amenós Vidal](#) el 11 Nov 2010 - [URL Permanente](#)

Selección del explorador.

Nuestra recomendación siempre ha sido utilizar Internet Explorer 8 como navegador, por sus características en cuanto a seguridad. Sin embargo, después de meses de utilización hemos encontrado el primer problema que experimenta este explorador en comparación a otros.

El ejemplo que ahora ponemos nos ha obligado a utilizar una etiqueta "meta" en el código fuente html de la página electrónica que deseamos visualizar con IE8 para evitar problemas que no surgen en cambio con los demás navegadores.

Hemos comprobado el buen funcionamiento en Avant, Maxthon, Mozilla Firefox, Safari, Opera, Netscape o Google Chrome, y aunque Internet Explorer 7 responde bien, con la versión 8 más reciente de actualización experimentamos conflictos. Si combinamos varios reproductores de vídeo en una sola página electrónica, de modo que dependen de varios scripts e iframes para su uso, se bloquea la reproducción.

Si este es su problema, comprobando la correcta configuración del código fuente html de su web, de modo que al usar Internet Explorer 7 y 8, todos los textos e imágenes se ven en el mismo sitio, y el único problema es que el primero reproduce simultáneamente todos los vídeos en sus distintas ubicaciones, pero el segundo, se colapsa en el momento de la reproducción, esta es la solución que busca.

Simplemente deberá introducir el siguiente código fuente entre las etiquetas <head> y </head> del oficio de encabezamiento, y sus problemas se habrán solucionado.

```
<meta http-equiv="X-UA-Compatible" content="IE=7" />
```

Esta etiqueta "meta" la utiliza Windows Live, MSN y otros sitios en Internet de Microsoft, que activa automáticamente en IE8 la vista de compatibilidad del menú de herramientas, evitando el conflicto mencionado al igual que otros exploradores no lo experimentan.

Compartir

[Me gusta](#) [Regístrate para ver qué les gusta a tus amigos.](#)

[Twitter](#) (0)

[0 comentarios](#)

Tags: [mozilla firefox](#), [internet explorer](#), [maxthon](#), [google](#), [safari](#), [opera](#), [avant](#), [windows](#), [netscape](#), [microsoft](#), [webmaster](#)

[Leer siguientes »](#) [« Leer anteriores](#)

## Networkers

webmasters

15 Oct 2010

### Códigos .htaccess para desarrolladores

Escrito por: [Carmen Martínez Ibáñez](#) el 15 Oct 2010 - [URL Permanente](#)

La configuración del archivo .htaccess (hypertext access) de Apache puede resultar ser una herramienta muy segura en el desarrollo web si se utiliza de forma adecuada. Con .htaccess podemos:

- I. Bloquear spammers, hackers, etc. ...
- II. Evitar robots y otros sitios no seguros ...
- III. Crear listas de IPs prohibidas.
- IV. Evitar navegaciones maliciosas.

Los códigos básicos para mejorar la seguridad de un sitio web, pueden ser extraídos de la guía rápida y breve sobre como introducir código específico y genérico contra la infección en el servidor, que puedes encontrar en nuestro manual sobre Internet y Seguridad. [Pulse aquí](#).

Pero antes de proceder a aplicar algunos cambios, debes hacer un backup del archivo (y es más, os recomendamos que en la medida de lo posible, los cambios efectuados los probais a nivel de host local antes de subirlos al servidor).

Compartir       

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 Twitter 

 0 comentarios Tags: [anti malware](#), [networkers](#) [comunity](#), [webmaster](#), [htaccess](#), [apache](#)

12 Oct 2010

### Botnets y diagnóstico de IPs

Escrito por: [José María Amén de Vidal](#) el 12 Oct 2010 - [URL Permanente](#)

#### Zombie Detection System + SpamHaus

ZDS - Zombie Detection System de PineApp Ltd. (Israel) empresa líder en seguridad de redes, es un sistema de detección único para identificar si la IP (Internet Protocol) de tu computador personal o servidor forman parte de una red de ordenadores zombies o botnet.

Hasta un 80 % del correo no deseado viene o bien en botnets que pueden ejercer un control remoto y automatizado de su computador convirtiendo su PC en una fuente potencial de spam.

SH - SpamHaus Project Ltd. de UE - Unión Europea comprueba las direcciones IP en listas negras o blancas (blacklists + whitelists): SBL (Spamhaus block list), XBL (Exploits block list), PBL (Policy block list), etc. ...

Compartir       

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 Twitter 

 0 comentarios Tags: [pineapp](#), [spamhaus](#), [ip](#)

11 Oct 2010

### Más sobre cibercriminales y botnets fraudulentas ...

Escrito por: [José María Amén de Vidal](#) el 11 Oct 2010 - [URL Permanente](#)

#### La gallina de los huevos de oro clandestina.

Los cibercriminales ya no se conforman sólo con sus datos. Ahora su equipo es lo que se subasta.

Autor: Robert Lemos (\*)

Fuente: [Norton Cybercrime News](#).

Fecha: 11/10/2010.

Asiduamente, los criminales cibernéticos compran e intercambian la información personal y financiera de sus víctimas. No obstante, los investigadores de seguridad se están dando cuenta de que los ladrones online están expandiendo su negocio ilegítimo más allá de la venta de datos. Ahora, están vendiendo acceso a su equipo.

En junio, la firma de seguridad web Finjan comunicó que sus investigadores habían encontrado una plataforma de comercio online que permitía a los compradores criminales alquilar o adquirir bloques de sistemas afectados, comúnmente denominados bots o zombies. El intercambio criminal, al que sus creadores denominaron "Golden Cash", representa una manera sencilla para los cibercriminales de obtener ganancias a través del control de los sistemas de sus víctimas.

Este servicio, que ha desaparecido desde que fue descubierto, tenía el objetivo de ser un recurso integral para las necesidades de un cibercriminal, explica Yval Ben-Itzak, Gerente de tecnología de Finjan.

"Uno puede dirigirse ahí y comprar tantos equipos infectados como desee", agrega. "Luego, puede configurar los sistemas como desee, simplemente utilizando ese sitio".

Estos servicios pueden representar un negocio lucrativo para sus propietarios. En el momento del informe, el sitio Golden Cash pagaba a su partners entre 5 y 100 dólares por un bloque de 1.000 equipos infectados. Los precios varían, con los sistemas de China, Taiwán, Corea del Sur y Filipinas entre los más baratos, y los de Australia entre los más caros. Así, los compradores pueden "adquirir" los sistemas por precios que varían desde los 20 dólares hasta los 500 por 1.000 bots, según la ubicación. Como los compradores pueden utilizar los sistemas y volver a venderlos cuando hayan terminado, la cantidad de bots disponibles se actualiza continuamente.

"Los mismos equipos se comercializan una y otra vez y los utilizan diferentes personas", comenta Ben-Itzak. "Uno puede adquirirlo y utilizarlo para siempre o utilizarlo sólo por una semana.

#### Evolución, no revolución.

Como muchos negocios lucrativos, la red Golden Cash no es una tecnología completamente nueva, sino una combinación de modelos comerciales que han funcionado bien en internet.

En el pasado, por ejemplo, los cibercriminales con grandes botnets segmentaban el grupo de equipos en redes más pequeñas que podían vender. No obstante, Golden Cash ha mejorado ese sistema al permitir a los compradores no sólo escoger el tamaño de su botnet, sino también personalizar el software para esos sistemas.

"Creo que estamos siendo testigos de una evolución", dice Ben-Itzak.

Los criminales obtienen un margen de cada intercambio, por lo que el intercambio continuo de un número cada vez mayor de bots por parte de sus clientes aumenta las ganancias, agrega.

Los cibercriminales también descubrieron que intentar gestionar botnets de cientos de miles (o millones) de equipos afectados era una pesadilla. En lugar de un único botnet de un millón de equipos, 100 redes de 10.000 sistemas cada una resulta más lógica, explica Vincent Weafer, Vicepresidente del grupo Security Response de Symantec.

"Hemos visto sitios web alojados, la formación de grupos de afiliados y el pago por clics", agrega Weafer. "Todo esto ha existido durante varios años, pero Golden Cash lo ha combinado".

#### Comercio de esclavos digitales.

Mantener sus sistemas lejos del bloque de subastas digitales no es sencillo. Los cibercriminales, o sus partners, conocidos como afiliados, ponen en peligro incluso sitios web conocidos con códigos que pueden utilizarse para infectar los equipos de los consumidores desprevenidos.

Por ejemplo, la primera actividad del troyano Golden Cash después de haber infectado el equipo de una víctima es buscar nombres de usuarios y contraseñas que permitan el acceso a servidores de archivos. Con esas credenciales, los criminales cibernéticos pueden continuar tomando el control de los servidores web y los sitios alojados en esos servidores. En su investigación, Finjan descubrió una memoria caché de nombres de usuarios y contraseñas de más de 100.000 sitios.

"Estas credenciales se utilizan con posterioridad para permitir a sus partners introducir código malicioso en las páginas web", explica el informe, y agrega que "se identificaron dominios corporativos de todo el mundo en esta lista".

En algunos casos, entre los estafadores se incluye código malicioso en anuncios publicitarios online falsos que luego distribuyen los servicios publicitarios para que aparezcan en diferentes sitios web.

Los sitios web populares no son inmunes a estos ataques. A principios de septiembre, la edición online de New York Times alojó varios anuncios publicitarios con códigos de ataque. CNN, ZDNet, Yahoo e incluso algunos sitios de empresas de seguridad han alojado código malicioso de diferentes maneras.

El resultado: los equipos de los consumidores que visitan sitios web legítimos que albergan anuncios publicitarios maliciosos pueden ser infectados con esclavos de códigos no autorizados y ser vendidos en sitios de intercambio clandestino, como Golden Cash.

#### El ciclo del crimen.

El negocio de vender bots tiene su propio ciclo, el cual comienza con el afiliado. Los afiliados se registran para recibir el servicio de Golden Cash e infectar los equipos de las víctimas con un troyano personalizado, y ganan dinero por cada equipo que el software pone en peligro.

Una vez que el visitante no deseado infecta un sistema informático, la primera orden es obtener los nombres de usuario y las contraseñas de los sitios web que el usuario del sistema utiliza.

Luego, el sistema informático de la víctima se vuelve parte del grupo de bots esclavizados y, tarde o temprano, se ofrece a otros delincuentes online que utilizan el sitio web dedicado. Los equipos con base en el Reino Unido, Australia y los países europeos son más vulnerables que los de África y Asia, dice Weafer.

"El pago varía entre uno o dos centavos (por sistema) y cincuenta centavos", agrega. "Todo depende de la ubicación de los activos".

Las ganancias de estas estafas ilegales pueden ser enormes. Los afiliados pueden obtener millones de dólares infectando los equipos de consumidores con código malicioso Golden Cash o de otro tipo. El investigador de seguridad Dmitry Samosenko, de la firma antivirus Sophos, encontró una captura de pantalla online que mostraba que un afiliado ganaba casi 6.500 dólares al mes gracias a una estafa con un reproductor de vídeo falso. Otro servicio para cibercriminales hacía alarde de que uno de sus socios ganó casi 5.000 dólares en once días, según escribió el investigador en una nota publicada en septiembre.

"Suponiendo que la mayoría de los administradores de sitios web dirigen el tráfico a más de un patrocinador por vez, no sorprende que el marketing de los afiliados (y otras técnicas) sea un área profesional muy tentadora para un experto en equipos en Europa del Este", escribió.

(\*) Robert Lemos es un premiado periodista especializado en tecnología con más de 13 años de experiencia en la resolución de problemas de seguridad de equipos, cibercrimen y seguridad empresarial. El trabajo de Lemos ha sido publicado en BusinessWeek, San Francisco Chronicle, SecurityFocus, PC Magazine, PCWorld, USA Today, Wired News, Technology Review, ZDNet y en sitios web como CNET News, CIO y The New York Times.

Compartir       

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 Twitter 

 0 comentarios Tags: [security response](#), [norton](#), [finjan](#), [symantec](#), [sophos](#)

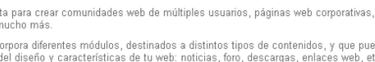
26 Sep 2010

### XOOPS 2.0 - Content Management System

Escrito por: [José María Amén de Vidal](#) el 26 Sep 2010 - [URL Permanente](#)

Fuente: [Xoops](#)

Xoops 2.0 proporciona un servidor virtual FTP - File Transfer Protocol, y relacional de base de datos SQL (Structured Query Language) que dispone de varios módulos de seguridad y mantenimiento que garantizan la protección del CMS (Content Management System). [Pulse aquí](#).



#### Potente, flexible y completo sistema de gestión de contenidos

Autor: Elena Santos.

Xoops es lo que se denomina un sistema de administración de contenidos web, mediante el cual el administrador de un sitio web puede fácilmente crear páginas web dinámicas, con gran control de gestión de contenidos, y (...) otras interesantes funcionalidades.

Resulta perfecta para crear comunidades web de múltiples usuarios, páginas web corporativas, weblogs personales y mucho más.

El sistema incorpora diferentes módulos, destinados a distintos tipos de contenidos, y que puedes utilizar o no en función del diseño y características de tu web: noticias, foro, descargas, enlaces web, etc. ...

Xoops utiliza una base de datos relacional (MySQL), permite a sus usuarios registrados un altísimo nivel de personalización de la página web, permite el uso de temas de diseño (...) y es totalmente gratuito, gracias al trabajo de toda una comunidad que lo desarrolla y mejora día a día bajo la licencia GNU.

Compartir       

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 Twitter 

 0 comentarios Tags: [webmaster](#), [xoops](#), [gnu](#)

12 Sep 2010

### Herramientas para webmasters de Google

Escrito por: [Carmen Martínez Ibáñez](#) el 12 Sep 2010 - [URL Permanente](#)

Fuente: [Google](#).

La instrumentalización de las herramientas para webmasters de Google, te brinda informes detallados acerca de la instrumentalización y mejora de tu sitio en los resultados de búsqueda. [Pulse aquí](#).

Para comenzar, añade y verifica tu sitio a través de la inserción de códigos "meta" e inmediatamente comenzarás a ver información. Obtén el punto de vista de Google y diagnóstica los errores. Conoce el mecanismo para su rastreo e indexación, así como los problemas específicos que experimentamos para acceder a él.

Visualiza, clasifica y descarga información complementaria acerca de los enlaces externos y internos. Descubre las consultas que generan tráfico y la ruta que siguen exactamente los usuarios.

Comparte información y envía comentarios sobre tus páginas a través de sitenaps (xml) y/o robots (txt), cuáles son las más importantes y con qué frecuencia cambian.

También puedes solicitar la comprobación de la web a través de su página de diagnóstico de navegación segura, con el fin de confirmar que tu sitio en Internet está libre de malware y no ha distribuido software malicioso en los últimos 90 días.

#### Google Webmaster Help.

Autor: Juan Manuel González.

El servicio de ayuda del Centro para Webmasters está disponible en 12 idiomas, incluyendo francés, italiano, alemán, español, portugués y ruso, está pensado como un lugar de encuentro para que los usuarios se ayuden entre ellos, hagan preguntas y compartan información sobre cómo Google rastrea e indexa los sitios web. En ocasiones participará el equipo de Google. [Pulse aquí](#).

Compartir       

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 Twitter 

 0 comentarios Tags: [anti malware](#), [google](#), [webmaster](#)

31 Ago 2010

### Google Safe Browsing + Malware Domain List

Escrito por: [José María Amén de Vidal](#) el 31 Ago 2010 - [URL Permanente](#)

Fuente: [Google](#)

Una herramienta para webmasters de gran utilidad para los internautas es la página de diagnóstico de navegación segura de Google safe browsing que combinada a la lista de dominios maliciosos de Malware domain list nos ofrece una buena manera de distinguir los sitios seguros e inseguros.

El funcionamiento consiste en añadir la dirección electrónica de cualquier sitio en Internet que queramos diagnosticar a la url de Google safe browsing, por ejemplo, del dominio [malwaredomainlist.com](#) que nos ofrece dicha lista de dominios maliciosos. [Pulse aquí](#).

Del siguiente modo:

<http://www.google.es/safebrowsing/diagnostic?site=malwaredomainlist.com>

Es un buen modo, para determinar los sitios legítimos y/o que han sido víctimas de inyección de código malintencionado por servidores remotos que contienen dominios maliciosos.

Compartir       

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 Twitter 

 0 comentarios Tags: [anti malware](#), [malware domain list](#), [google](#), [webmaster](#)

26 Ago 2010

### SafeSearch de Google

Escrito por: [Carmen Martínez Ibáñez](#) el 26 Ago 2010 - [URL Permanente](#)

Fuente: [Google](#).

Al utilizar el buscador de Google, para poder filtrar los resultados obtenidos como medida de seguridad, para ello debe marcar la opción del menú de configuración de búsqueda.

#### Bloqueo.

El formulario de preferencias globales muestra el filtro de control general mediante la aplicación de la función de bloqueo SafeSearch, que permite un equipo filtrado en todas las búsquedas realizadas en su equipo con el navegador que utiliza habitualmente.

Si no ha accedido a su cuenta de Google, se le solicitará que acceda, y si no dispone de una deberá crearla. Una vez que haya accedido, se le solicitará que marque el botón de bloqueo. Este último paso tarda algunos minutos en realizarse, ya que el filtro estricto se aplica a todos los dominios de Google.

Una vez que se haya activado el bloqueo, aparecerá una página de confirmación, de manera que si el bloqueo de SafeSearch está activado, la parte superior de la página de resultados se verá de forma distinta, con un mensaje junto al cuadro de búsqueda y su logotipo, que se mostrarán en la parte derecha.

#### Verificación.

Una vez completado el proceso, es posible verificarlo con el fin de confirmar que esta función sigue activa para poder aplicar un filtro estricto en todos los dominios de Google, de modo que se vuelve a bloquear cualquier dominio nuevo o que se haya desbloqueado.

#### Sugerencias.

- Si dispone de varios navegadores en el equipo, debe establecer el bloqueo en cada uno de ellos de forma individual.
- Si el equipo dispone de varios perfiles de usuario, debe establecer el bloqueo en cada perfil.
- Asegúrese de que el navegador esté configurado para permitir cookies.

Compartir       

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 Twitter 

 0 comentarios Tags: [safesearch](#), [google](#), [webmaster](#)

23 Ago 2010

### Yahoo + Majestic SEO

Escrito por: [Carmen Martínez Ibáñez](#) el 23 Ago 2010 - [URL Permanente](#)

Nos interesa especialmente este motor de búsqueda puesto que estrategia info dispone de un SEO - Search Engine Optimization (backlinks discovery) mejor posicionado en comparación con los diferentes buscadores de Internet (Google, AOL, ASK, Lycos, etc. ...). [Pulse aquí](#).



Compartir       

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 Twitter 

 0 comentarios Tags: [seo](#), [yahoo](#), [webmaster](#)

12 Ago 2010

### Dasient WAM - Web Anti-Malware

Escrito por: [José María Amén de Vidal](#) el 12 Ago 2010 - [URL Permanente](#)

Fuente: [Dasient](#)

Un buen programa para la prevención de intrusiones en sitios legítimos, es Dasient Web Anti-Malware que desarrolla la misma tecnología que utiliza Google para detectar en la red los sitios que distribuyen software malicioso (intencionado o no). [Pulse aquí](#).

#### Ex trabajadores de Google crean un servicio que reduce el malware de las webs.

Autor: Arancha Asenjo y Marta Cabanillas.

La start-up Dasient se estrena con un servicio basado en cloud diseñado

## Networkers

Webmasters

20 Jul 2010

### VirusList + Removal Tool de Kaspersky

Escrito por: [José María Aménos Vidal](#) el 20 Jul 2010 - [URL Permanente](#)



Fuente : [Kaspersky Lab](#).

VirusList.com todo sobre seguridad en Internet es un sitio oficial de Kaspersky.com, compañía de software de seguridad que ofrece toda la información actualizada sobre alertas y amenazas en la red destacables (virus, troyanos, ...) , ataques informáticos recientes (hackers, spam,...), últimos parches de seguridad (Microsoft, Adobe, ...) así como otras muchas noticias de interés para usuarios, webmasters y programadores.

Señalamos por su importancia el informe trimestral que aparece periódicamente, el último fue publicado con fecha 1 de junio del 2010, y que trata sobre el desarrollo de las amenazas informáticas en el primer trimestre del año. [Pulse aquí](#).

Kaspersky Virus Removal Tool se trata de un programa de análisis exhaustivo y profundo de su ordenador con el fin de localizar posibles infecciones por malware en general, que no ofrece protección residente o en línea, pero que es un potente rastreador.

Autoscan con una velocidad de procesamiento alrededor de un millón de archivos analizados en más de 10 h. no es uno de los componentes más rápidos del mercado, aunque dispone de un extenso proceso de análisis, amplias listas de virus y bases de datos sobre firmas de intrusiones, que lo hacen más que recomendable por su capacidad de encontrar en ubicaciones remotas aquellos objetos y ficheros infectados o sospechosos que no detectan otros productos.

La descarga y configuración es sencilla, se instala o desinstala automáticamente tras solicitar su ejecución, lo que hace de este componente de software un sistema inteligente, trabaja sin conexión a la red, finaliza sus análisis con un informe detallado de incidencias, y con el fin de no afectar al rendimiento de su procesador cuando realice otras tareas programadas procede a desinstalarse en modo automático previa solicitud. [Pulse aquí](#).

Compartir

Me gusta Registrado para ver qué les gusta a tus amigos.

0

0 comentarios

Tags: [anti malware](#), [anti spyware](#), [viruslist](#), [kaspersky](#)

03 Jul 2010

### Hispasec Sistemas y análisis de VirusTotal

Escrito por: [José María Aménos Vidal](#) el 03 Jul 2010 - [URL Permanente](#)



Fuente : [Hispasec Sistemas](#).

VirusTotal es un servicio de análisis de archivos sospechosos que permite detectar virus, troyanos, y malware en general, que ha sido premiado por la edición americana de la revista PC World como uno de los 100 mejores productos del año 2007 en la categoría Security Web Site.

Características.

- Servicio independiente y gratuito.
- Uso simultáneo de múltiples motores antivirus.
- Actualización automática de los motores en tiempo real.
- Resultados detallados por cada uno de los antivirus.
- Estadísticas globales en tiempo real.

Créditos.

Un servicio desarrollado por Hispasec Sistemas, laboratorio independiente de seguridad informática, que utiliza las versiones en línea de comando de varios motores antivirus, actualizados puntualmente con las firmas oficiales publicadas por sus desarrolladores.

VirusTotal no sustituye de forma alguna a los antivirus instalados en los PCs, ya que sólo permite el análisis a demanda de archivos individuales, y no ofrece protección permanente al sistema del usuario, aunque el índice de detección ofrecido por el análisis simultáneo de múltiples motores antivirus es muy superior al de un solo producto. [Pulse aquí](#).

Compartir

Me gusta Registrado para ver qué les gusta a tus amigos.

0

0 comentarios

Tags: [hispasec sistemas](#), [virustotal](#)

14 Jun 2010

### Comentarios sobre Adobe Digital Editions y Microsoft Reader

Escrito por: [Carmen Martínez Ibáñez](#) el 14 Jun 2010 - [URL Permanente](#)

Fuente : [Adobe & Microsoft Reader](#).

Aunque no es reciente, puesto que este tipo de lectores de e-books ya tienen desde 2002-03 bastante utilización en el mundo editorial, comentarios los más importantes y a los que dedicamos nuestra atención, son [Adobe Digital Editions](#) y [Microsoft Reader](#).

Con independencia del más conocido formato pdf de Adobe Reader, por ejemplo los ficheros .epub tienen mucha aceptación en el campo de las ventas de libros en formato digital. [Pulse aquí](#).

Y en cuanto al más clásico lector electrónico de Microsoft Reader, se puede descargar [Pulse aquí](#).

Es conveniente que dispongan como mínimo en sus computadoras de estos 2 lectores, por ser los más utilizados y que prometen extenderse mucho más a partir de ahora y en el futuro.

Con este propósito hemos obtenido la Microsoft Reader Publisher + ISV Licensing. [Pulse aquí](#).

## Certificate

### Commercial Use License Agreement

Compartir

Me gusta Registrado para ver qué les gusta a tus amigos.

0

0 comentarios

Tags: [adobe](#), [microsoft](#)

08 Jun 2010

### CMS Xoops : Módulos de seguridad y mantenimiento

Escrito por: [José María Aménos Vidal](#) el 08 Jun 2010 - [URL Permanente](#)

XOOPS es una de las plataformas más conocidas en la red de freeware y shareware, software libre y gratuito con licencia OSI - Open Source Initiative para la implementación de CMS (Content Management System), sistema de administración de contenidos que utiliza Apache, FTP, MySQL, etc ... principalmente enfocado a la creación de sitios o portales web para comunidades virtuales en Internet, y que dispone de una amplia gama de aplicaciones y complementos de actualización.

A continuación destacamos las herramientas de administración que hacen referencia a seguridad del sistema, gestión y mantenimiento de la base de datos, componentes básicos que los webmasters deben configurar una vez instalados en la carpeta de módulos CMS Xoops de su servidor FTP (File Transfer Protocol).

#### Herramientas de administración

##### Seguridad del sistema

###### Indexscan 2.03

Basicamente destacamos como más importante el examen de archivos index.html perdidos y su recuperación, o el rastreo y localización de inyecciones iframes, con la posibilidad de elaborar informes de estado. [Descargar](#).

###### Protector 3.4

Una central de protección con manual de seguridad para cierres forzados de sesión hijacking, expulsiones y basados de IP en caso de ataques DNS, FS, spam e inyección SQL, control de wrapping sospechoso y crawler malicioso, contraseñas de reparo, etc ... [Descargar](#).

###### Xortify 1.16

Aplicación para fortalecer la seguridad de red y que utiliza técnicas de Web 2.0 para evitar intrusiones, incluye la notación exacta del intruso y previene de cualquier ataque. Es un acceso necesario y protector al estilo de un firewall. [Descargar](#).

##### Mantenimiento de la base de datos.

###### Xoopscore 1.22

Un módulo diseñado para ayudar a mantener de forma automática su sitio web, del que destacamos la opción de verificar, reparar, analizar y optimizar su base de datos. [Descargar](#).

###### XOOPS DB Backup & Restore 3.0

Es una sencilla herramienta que permite entre otras prestaciones, hacer una copia de seguridad o el backup de la base de datos en formato de archivos comprimidos y/o SQL ... [Descargar](#).

Compartir

Me gusta Registrado para ver qué les gusta a tus amigos.

0

0 comentarios

Tags: [webmaster](#), [xoops](#), [osi](#)

01 Jun 2010

### Norton Safe Web y McAfee Site Advisor

Escrito por: [José María Aménos Vidal](#) el 01 Jun 2010 - [URL Permanente](#)

Norton Safe Web y McAfee Site Advisor son herramientas de gran utilidad para webmasters y usuarios, que resultan ser a día de hoy el mejor modo de evaluar la seguridad de un sitio web en la red.

Ambos sistemas disponen de formularios en línea para el análisis de riesgos que hemos aplicado a estrategia info para mostrar sus resultados.

**Norton Safe Web** indica el nivel de amenazas para su equipo e identidad y que se detalla por virus heurísticos, programas de descargas no autorizadas o maliciosas, aplicaciones sospechosas, troyanos y spyware, publicidad no deseada, ataques de phishing, puertas traseras o software de acceso remoto, sustracción de información u otros riesgos. Para más información útil sobre amenazas. [Pulse aquí](#).



**McAfee Site Advisor** muestra los resultados de la prueba de seguridad web automatizada para el correo electrónico, con un análisis de descargas detallado, una muestra de afiliaciones en línea o vínculos a sitios seguros, así como otros contenidos de revisión sobre software publicitario, espía u otros programas no deseados, spam, phishing y otras estafas, elementos emergentes y vulnerabilidades. Para ver el informe del sitio. [Pulse aquí](#).

Compartir

Me gusta Registrado para ver qué les gusta a tus amigos.

0

0 comentarios

Tags: [norton](#), [mcafee](#), [webmaster](#)

30 May 2010

### Selección del explorador

Escrito por: [Carmen Martínez Ibáñez](#) el 30 May 2010 - [URL Permanente](#)

El explorador es un importante componente de software para su equipo, se utiliza para navegar por Internet y abrir los sitios web que visita. Hay varios exploradores disponibles y cada uno de ellos con variadas características.

En la siguiente lista se muestran los más utilizados. Se indican los enlaces a hipervínculos para el correo de instalación e información adicional para su selección. Nuestra recomendación es IE - Internet Explorer 8.

**Avant** Diminuto, rápido, simple, altamente configurable y extensible. [Descargar](#).

**Google Chrome**. Un nuevo navegador de Google, más rápido y sencillo. [Descargar](#).

**Internet Explorer**. Use en herramientas la "vista de compatibilidad" y controle su privacidad. Diseñado por Microsoft. [Descargar](#).

**Maxthon** Bloqueador de anuncios y ganador dos veces de los Premios Webware. [Descargar](#).

**Mozilla Firefox**. Tu seguridad en Internet es la prioridad principal de Firefox. [Descargar](#).

**Netscape**. El clásico navegador de uso polivalente y multifuncional. [Descargar](#).

**Opera**. Seguro, potente, y con excelente protección de la privacidad. [Descargar](#).

**Safari**. Seguro de Apple para Windows, el navegador web más innovador del mundo. [Descargar](#).

Compartir

Me gusta Registrado para ver qué les gusta a tus amigos.

0

1 comentario

Tags: [internet explorer](#), [mozilla firefox](#), [avant](#), [google](#), [maxthon](#), [opera](#), [safari](#), [netscape](#)

29 May 2010

### RSS y CSS Validation Service

Escrito por: [Carmen Martínez Ibáñez](#) el 29 May 2010 - [URL Permanente](#)

W3C - World Wide Web Consortium pone a disposición de los webmasters un servicio en línea con el objetivo de validar los feeds de sindicación en sus formatos y verificar las hojas de estilo de las páginas electrónicas. Un test gratuito con licencia OSI - Open Source Initiative que comprueba la sintaxis de archivos y ficheros. A continuación los ejemplos de aplicación de RSS y CSS Validation Service para estrategia info con el código fuente de su validación y verificación.

#### Validar la sintaxis RSS

RSS - Really Simple Syndication.



<A href="http://validator.w3.org/feed/check.cgi?url=http://estrategia.info/fpc/rss.php" target= "blank"><IMG title="Validate my RSS" border=0 alt="Valid RSS]" src="http://estrategia.info/fpc/images/w3c-rss.png"></A>

XML - Extensible Markup Language.



<A href="http://validator.w3.org/feed/check.cgi?url=http://psicologos.estrategia.info/backend.php" target= "blank"><IMG title="Validate my RSS" border=0 alt="Valid RSS]" src="http://estrategia.info/fpc/images/w3c-rss.png"></A>

Verificar las hojas de estilo CSS.

CSS - Cascading Style Sheets.



<A href="http://jigsaw.w3.org/css-validator/validator?url=http://estrategia.info/fpc/themes/modern/style.css" target= "blank"><IMG title="Validate my CSS" border=0 alt="Valid CSS]" src="http://estrategia.info/fpc/images/w3c-css.gif"></A>

CMS - Content Management System.



<A href="http://jigsaw.w3.org/css-validator/validator?url=http://psicologos.estrategia.info/themes/classina\_blog/style.css" target= "blank"><IMG title="Validate my CSS" border=0 alt="Valid CSS]" src="http://estrategia.info/fpc/images/w3c-css.gif"></A>

Compartir

Me gusta Registrado para ver qué les gusta a tus amigos.

0

0 comentarios

Tags: [w3c](#), [osi](#), [webmaster](#)

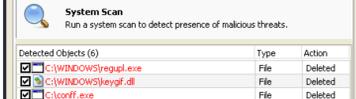
17 May 2010

### NoVirusThanks Malware Remover

Escrito por: [José María Aménos Vidal](#) el 17 May 2010 - [URL Permanente](#)

NoVirusThanks Malware Remover es una aplicación diseñada para detectar y eliminar malware genérico y específico (troyanos, virus, etc ...) u otras amenazas que pueden dañar su computadora. También incluye la posibilidad de eliminar spyware y adware. [Pulse aquí](#).

Lo recomendamos porque es un programa muy práctico y fácil de usar que escanea en tiempo real de forma rápida y no usa o necesita gran cantidad de memoria virtual, incluso se puede ejecutar junto a otras aplicaciones que consumen por su rendimiento altos recursos están funcionando.



#### Características principales.

- Método de desinfección.
- Quita programas y aplicaciones no deseadas.
- Elimina malware, spyware y adware.
- Quick Scan y Full Scan : análisis rápido y completo de registros, módulos y procesos.
- Copia de seguridad de archivos y carpetas.
- Manual para la actualización de base de datos.

Información sobre el producto.

- Probación de archivos.
- Sistema operativo : Windows.
- Idioma : multilingüe.
- Licencia : Freeware.

Compartir

Me gusta Registrado para ver qué les gusta a tus amigos.

0

0 comentarios

Tags: [anti malware](#), [anti spyware](#), [novirusthanks](#), [windows](#)

15 May 2010

### Advanced SystemCare : Programa de optimización para Windows

Escrito por: [Carmen Martínez Ibáñez](#) el 15 May 2010 - [URL Permanente](#)

Fuente : [iObit Software](#).

Advanced SystemCare, es un programa de optimización del sistema operativo, creado por iObit Software, empresa china con sede en Changdu, que limpia y mantiene el ordenador, analiza el rendimiento y los problemas de seguridad, e incluye otras utilidades para mejorar el rendimiento del sistema y el disco, proteger los datos y tener una seguridad óptima en el PC, así como para controlar el sistema de Windows. [Pulse aquí](#).



#### 1. Limpieza de Windows.

- Limpieza de spyware. Escanea y elimina el spyware y adware.
- Revisión del registro. Limpia el registro para mejorar el rendimiento.
- Limpieza de datos privados. Elimina tu historial y restos de internet u otros programas.
- Borrado de archivos. Borra los archivos temporales, recuperando espacio.

...

#### 2. Prevención y mejora.

- Sistema de optimización. Optimiza y repara la configuración del sistema.
- Inmunizar contra spyware. Previene el spyware en los archivos de tu PC.
- Desfragmentación de discos. Desfragmenta el disco para obtener mayor rendimiento.
- Análisis de seguridad. Escanea Windows para encontrar configuraciones hijacking.

...

#### 3. Utilidades. Herramientas adicionales.

- a. **Sistema**. Para mejorar el rendimiento del sistema y el disco.
  - Check Disk. Comprueba la estructura del disco reparando errores relacionados con sectores corruptos, clusters perdidos, ficheros cruzados y directores erróneos.
  - Disk Cleaner. Limpia el disco buscando ficheros innecesarios y recupera espacio en el disco.
  - Registry Defrag. Comprime y optimiza el registro eliminando las entradas innecesarias, reduciendo la fragmentación, corrigiendo errores estructurales y recuperando memoria sin usar.
  - Shortcut Fixer. Repara accesos directos.

...

#### b. Seguridad.

- Backup Genius. Supervisa y asegura el funcionamiento de los dispositivos, dispositivos, procesadores, etc ...
- IE Helper. Controla la seguridad de Internet Explorer.
- NBBackup. Restaura configuraciones del sistema y documentos, realizando una copia de seguridad.
- SFC. Comprueba los ficheros del sistema y valida la firma digital restaurando los incorrectos.

...

#### c. Otras.

- Auto Shutdown. Apagado o reinicialización automática y programada del PC.
- Disk Explorer. Explorador del disco.
- Restore Center. Centro de restauración.
- System Information. Información del sistema.

...

Compartir

Me gusta Registrado para ver qué les gusta a tus amigos.

0

0 comentarios

Tags: [tobit software](#), [anti spyware](#), [windows](#)

14 May 2010

### Acunetix Web Vulnerability Scanner

Escrito por: [José María Aménos Vidal](#) el 14 May 2010 - [URL Permanente](#)

#### Análisis de vulnerabilidades y auditoría de seguridad de su sitio web.

Acunetix Web Security Scanner es probablemente la herramienta de seguridad de más alto nivel que existe hoy en día para asegurar su sitio web.

Debe ser una prioridad para cualquier particular u organización poner su empeño, más alto nivel que conseguir que la red sea un lugar seguro por el que navegar, porque los hackers están concentrando todos sus esfuerzos en las variadas aplicaciones, por ejemplo en las basadas en carros de compra de las tiendas online, en los formularios y páginas de acceso, en los contenidos dinámicos, etc ... que se encuentran en línea las 24 horas del día, 7 días a la semana, cuyo control de los datos importantes no escapa a ellos porque suelen hacer todo lo posible por tener acceso directo a las bases de datos de los clientes.

Firewalls, SSL y servidores bloqueados pueden resultar inútiles contra el pirata, cualquier defensa a nivel de red de seguridad puede no proporcionar una total protección contra los ataques en el puerto 80, que tiene que permanecer abierto, y porque a menudo la plataforma de software es propensa a ser vulnerable.

Por esta razón, Acunetix comprueba automáticamente sus aplicaciones web para descubrir si es susceptible de inyección SQL, XSS u otras vulnerabilidades.



#### Programas.

La dirección electrónica en Internet de esta aplicación se puede descargar. [Pulse aquí](#)

Y en archivo adjunto el manual en inglés con los 8 pasos necesarios para el análisis de vulnerabilidades y auditoría de seguridad de sus sitios web, tras instalar el programa informático Acunetix. [Pulse aquí](#).

Para la lectura de los informes de análisis necesitan para su visualización del programa Report Viewer. [Pulse aquí](#).

#### Ejemplos.

En nuestro caso, tuvimos que corregir una alerta máxima de nivel 3 que nos obligó a eliminar el archivo imagemanager.php en nuestro CMS (Content Manager System) del subdominio psicologos.estrategia.info (que es donde empezaron los ataques de la piratería informática que sufrimos del 25 de junio al 3 septiembre 2009) puesto que su configuración representaba una elevada vulnerabilidad. En la actualidad, nuestros dominios y subdominios de estrategia.info muestran un nivel de riesgo "0".

## Networkers

### Webmasters

09 May 2010

## Editor de registro y restricciones del escritorio activo

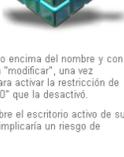
Escrito por: [José María Amenós Vidal](#) el 09 May 2010 - [URL Permanente](#)

En ocasiones puede ocurrir que después de un ataque por malware a su computadora se haya producido una modificación ajena a nuestra voluntad en el editor de registro, cambiando algunas propiedades, lo cual puede provocar una alerta de riesgo durante un examen de seguridad, por ejemplo con ParetoLogic Anti-virus PLUS en un sistema operativo Windows XP. En este caso, puede devolver a su estado original la configuración predeterminada, tal como se explica en el siguiente ejemplo y que es el más común que nos podemos encontrar.

Utilice el menú "Inicio" en el oficio de talonamiento de su monitor y desplegado marque la opción "ejecuta", continuación en la casilla en la que debe asignar el nombre del programa, carpeta, documento o recurso de internet que desea que Windows abra, debe poner "regedit.exe" y pulsar "Aceptar". Aparecerá entonces, el editor de registro.

En el menú izquierdo deberá abrir en este orden las siguientes carpetas y subcarpetas.

1. HKEY\_CURRENT\_USER.
2. Software.
3. Microsoft.
4. Windows.
5. CurrentVersion.
6. Policies.
7. ActiveDesktop.



El fichero que buscamos es "NoChangingWallpaper" que hay que editar, marcando encima del nombre y con el botón derecho del mouse se despliega una ventana en la que aparece la opción "modificar", una vez pulsada se visualiza la información del valor, al que debe asignar el número "1", para activar la restricción de configuración, puesto que el malware lo modificó situando en esta casilla la cifra "0" que la desactivó.

La necesidad de realizar esta operación estriba en restringir acciones remotas sobre el escritorio activo de su ordenador, porque en caso contrario, su política de privacidad se vería afectada e implicaría un riesgo de seguridad para su PC.

Compartir Me gusta Regístrate para ver qué les gusta a tus amigos.

0 comentarios

Tags: anti spyware, anti malware, paretoLogic, windows

07 May 2010

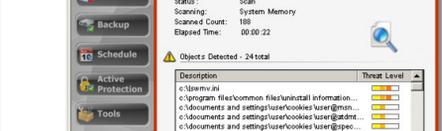
## ParetoLogic Anti-virus PLUS

Escrito por: [Carmen Martínez Ibáñez](#) el 07 May 2010 - [URL Permanente](#)

Fuente - ParetoLogic.

Cuidado con los ataques mediante archivos PDF.

Hoy en día los cibercriminales están utilizando métodos muy diferentes para poder entrar en su computadora y robar información personal como números de tarjetas de crédito, contraseñas, e información confidencial. Una forma muy común que trata de insertar malware en su sistema es utilizando las vulnerabilidades en archivos de Adobe Acrobat Reader que se pueden utilizar como una puerta de entrada para infectar su PC. Para detener estas amenazas existe un producto eficaz contra el virus y que es altamente recomendable.



Sugerimos ParetoLogic Anti-virus PLUS, que puede detectar, bloquear y limpiar estos virus. Instale las herramientas de seguridad y ejecute un examen personalizado, rápido o completo por si ha sido infectado por PDF exploits. [Pulse aquí.](#)

Nota : Para efectuar la eliminación manual de los archivos infectados que no se suprimen automáticamente mientras se realiza el examen de seguridad, puede seguir las mismas observaciones que recomendamos para ActiveScan Panda Security.

Revise la copia de seguridad de su página web, puesto que la bondad de este programa es encontrar códigos script maliciosos, que otros programas no localizan ... Para descarga directa de ParetoLogic Anti-virus PLUS ... [Pulse aquí.](#)

Después de instalado este anti-virus de última generación y tras el análisis, deben revisar en la sección Active Protection, el apartado blocked events que detalla una lista de archivos de su copia de seguridad que han sido bloqueados porque contienen código malicioso ... teniendo que sustituir por una copia de seguridad anterior a la infección, el archivo infectado en su ordenador.

ParetoLogic localiza generalmente scripts malintencionados en archivos login.php que hay que sanear ... [Pulse aquí.](#)

Compartir Me gusta Regístrate para ver qué les gusta a tus amigos.

0 comentarios

Tags: anti malware, anti spyware, paretoLogic, panda

05 May 2010

## AddOurSearch : Browser installer

Escrito por: [José María Amenós Vidal](#) el 05 May 2010 - [URL Permanente](#)

Addoursearch instala un buscador de contenidos en su navegador.



En caso de interesar la posibilidad de disponer de un buscador avanzado de contenidos publicados, además de los buscadores a su disposición mediante distintos proveedores de servicios (google, bing, yahoo, etc ...) también puede instalar en su PC directamente y en la barra de herramientas de su navegador, un buscador personalizado a su sitio web.

Instrucciones para webmasters.

AddOurSearch.com es un servicio gratuito que permite a los usuarios buscar en su sitio desde cualquier lugar en Internet, directamente a través de IE, Firefox, etc ... No hay necesidad de aprender códigos complicados o nuevos lenguajes, tan sólo debe rellenar un formulario con la información del sitio, luego copiar y pegar el código en su página web.

Siga las instrucciones que se indican a continuación. [Pulse aquí.](#)

Ejemplos para usuarios.



Una vez instalado el código, muestra por ejemplo el siguiente aspecto :

1. Marque la opción : Instalar.
2. En el cuadro de diálogo : ¿ Desea agregar el siguiente proveedor de búsquedas ?; pulsar agregar proveedor con la posibilidad de marcar la opción de convertirlo en predeterminado.

De este modo, junto a la barra de direcciones del navegador se habrá instalado en la lista de proveedores su nuevo buscador de contenidos, y para cualquier cambio puede usar la opción de cambiar las opciones predeterminadas de búsqueda.

Finalmente, introduzca un término y acceda a una de las dos opciones : notas de prensa o base de datos, y automáticamente aparecerán en la pantalla del monitor de su PC la lista de los artículos relacionados con la búsqueda seleccionada.

Compartir Me gusta Regístrate para ver qué les gusta a tus amigos.

0 comentarios

Tags: addoursearch, webmaster

30 Abr 2010

## SoloSEO : Check IndexRank

Escrito por: [Carmen Martínez Ibáñez](#) el 30 Abr 2010 - [URL Permanente](#)



Check IndexRank constituye una herramienta para webmasters que destaca por su utilidad al servir de índice de medición del volumen de Items que Google Search indexa en su buscador, en base a una estimación que se muestra por períodos (2 semanas, 1 mes, 3 meses, 6 meses, 1 año y el total).

Se basa en un algoritmo creado por SoloSEO que permita realizar calificaciones de nivel, mediante valores que oscilan del 1 al 10, de manera que una alta calificación expresa un mayor grado de indexación.

El procedimiento para evaluar el posicionamiento de cualquier sitio en la red es simple, se trata de ingresar el nombre de dominio que nos interesa evaluar en el formulario habilitado. Por ejemplo, el ranking para estrategia info es de 7 (30 de abril del 2010). [Pulse aquí.](#)

Compartir Me gusta Regístrate para ver qué les gusta a tus amigos.

0 comentarios

Tags: seo, webmaster

19 Abr 2010

## AddThis Social Bookmark & Share Button Widget

Escrito por: [Carmen Martínez Ibáñez](#) el 19 Abr 2010 - [URL Permanente](#)

AddThis Social Bookmark & Share Button Widget, es un gadget de aplicación a las redes sociales o networking. [Pulse aquí.](#)

1. Seleccione website, wordpress, blogger o myspace.
2. Solicite el tipo de botón.
3. Establezca los permisos de público o privado, según su preferencia (con o sin registro).
4. Obtenga el código html a copiar en su sitio en Internet.



Ver ejemplos en el oficio de encabezamiento del Coordinador y Grupo de Internet y Seguridad : WAM - Web Anti-Malware en Networkers Community, o la comunidad de bloggers del diario El País. [Pulse aquí.](#)

Compartir Me gusta A una persona le gusta una página. Regístrate para ver qué les gusta a tus amigos.

0 comentarios

Tags: networkers community, webmaster, addthis

26 Mar 2010

## 7 BYMC - Blogs y Medios de Comunicación 2010

Escrito por: [Carmen Martínez Ibáñez](#) el 26 Mar 2010 - [URL Permanente](#)

Ver / descargar : Se ha enviado la siguiente propuesta para presentar en la modalidad de flash talks de la presente edición de las Jornadas de Blogs y Medios de Comunicación, a celebrar el 15 y 16 de abril en Granada (España).

Título : Internet y Seguridad (\*)

Autor : José María Amenós Vidal.

Acreditación : Coordinador del grupo WAM (Web Anti-malware) de Networkers Community (NC).

**Blog** : En la sección de Tecnología, apartado de Internet, de la comunidad de bloggers en el diario El País.

Para más información sobre inscripciones y participación, puede rellenar el formulario habilitado al efecto y/o enviar sus propuestas por correo electrónico, consultando las bases en la página oficial del evento BYMC 2010.

(\*) El contenido de la comunicación, es accesible en el siguiente archivo adjunto. [Pulse aquí.](#)

El evento, se celebra en la sede de la Asociación de Prensa y cuenta con la colaboración de la Universidad de Granada (España).

Compartir Me gusta Regístrate para ver qué les gusta a tus amigos.

0 comentarios

Tags: networkers community, anti malware, bymc, webmaster

16 Mar 2010

## Declaraciones de Panda Labs sobre la botnet que afectó a 13 millones de usuarios en 190 países y 31.901 ciudades

Escrito por: [José María Amenós Vidal](#) el 16 Mar 2010 - [URL Permanente](#)

Fuente - Panda Security.

Tras la reciente desarticulación de la botnet intervenida bajo el mando operativo conjunto de Panda Security, Defence Intelligence, FBI y la Guardia Civil española (\*), que ha dado como resultado la detención de tres personas, y a través de la diferente información recopilada de la conocida trama, se ha descubierto que los 13 millones de ordenadores infectados con el bot están distribuidos en 190 países y en 31.901 ciudades diferentes.

Según Luis Corrons, director Técnico de Panda Labs, "los mayores ratios de infecciones los encontramos en países donde hasta ahora la educación de los usuarios en materia de seguridad informática y prevención no ha sido una prioridad. En cambio, otros países donde sí se están realizando este tipo de campañas en los últimos años, el nº de infecciones ha sido mucho menor, como es el caso de EE.UU., Alemania, UK o Japón".

El ranking de infecciones por ciudad está encabezado por Seúl, con un 5,36% de las IPs comprometidas; seguido por Bombay, con un 4,45%, y por Nueva Delhi, con el 4,27%. El top 20 es el siguiente:

- 1 Seúl 5,36%
- 2 Bombay 4,45%
- 3 Nueva Delhi 4,27%
- 4 México 3,89%
- 5 Bogotá 2,68%
- 6 Lima 1,98%
- 7 Kiev 1,68%
- 8 Bangalore 1,39%
- 9 Islamabad 1,24%
- 10 Teherán 1,23%
- 11 Kuala Lumpur 1,16%
- 12 Madrid 1,11%
- 13 Santiago de Chile 1,03%
- 14 El Cairo 1,01%
- 15 Hyderabad 0,82%
- 16 Santo Domingo 0,75%
- 17 Río de Janeiro 0,75%
- 18 Riad 0,72%
- 19 Medellín 0,65%
- 20 Dubái 0,63%



En cuanto a países, el ranking lo encabeza India, con el 19,14% de las infecciones; seguido por México, con el 12,95%, y Brasil, con el 7,74%. El top 20 de países afectados es el siguiente:

- INDIA 19.14
- MEXICO 12.95
- BRASIL 7.74
- COREA 7.24
- COLOMBIA 4.94
- RUSIA 3.14
- EGIPTO 2.99
- MALASIA 2.86
- UCRANIA 2.69
- PAKISTAN 2.55
- PERU 2.42
- IRAN 2.07
- ARABIA SAUDI 1.85
- CHILE 1.74
- KAZAKHSTAN 1.38
- EMIRATOS ARABES UNIDOS 1.15
- MARRUECOS 1.13
- ARGENTINA 1.10
- ESTADOS UNIDOS 1.05
- (...)



\*Gracias a la colaboración de las diferentes partes implicadas (...), el día 23 de diciembre a las 5:00 pm (GMT +1), dejamos sin servicio los servidores a los que se conectaba la botnet y redireccionamos las peticiones a un servidor controlado por nosotros. Es en este momento cuando vimos la cantidad de IPs diferentes y únicas que estaban siendo controladas por el bot, casi 13 millones, y cuando tuvimos acceso a la información que nos da las cifras de los países y ciudades afectadas", continúa Luis Corrons.

Y añade: "Entre estas IPs hay tanto ordenadores de usuarios particulares como de empresas. Al dibujar en un mapa los países afectados, esto es el resultado que nos da".

El Instituto de Tecnología de Georgia ha publicado una animación en la que se muestra el progreso de la infección de la botnet. David Dagon, "Ph.D. Candidate" del Instituto de Tecnología de Georgia, comenta sobre la distribución geográfica: "Creo que un aspecto destacable de esta botnet es que es diferente a lo que siempre se comenta sobre infecciones. Normalmente, la prensa suele publicar que los botmasters de países del Este atacan a países occidentales. (Por ejemplo los botmasters rusos y víctimas de la Unión Europea o de Estados Unidos). En estas ocasiones vemos lo contrario: botmasters de occidente, y víctimas del Este. La lección es muy clara: todos estamos ante una amenaza común".

Desde Panda Security recomendamos a todos los usuarios – ya sean particulares o empresas - que analicen en profundidad su PC para asegurarnos que no tienen el bot ... Para ello, pueden utilizar la aplicación online y gratuita ActiveScan (. . .)

(\*) Grupo de Delitos Telemáticos (GDT) de la Guardia Civil y la Brigada de Investigación Tecnológica (BIT).

Ver los siguientes artículos relacionados que a continuación se indican :

- Defence Intelligence de Canadá detecta la botnet responsable de los ataques malware en la red.
- Gadgets INFEX + ActiveScan de Panda Security.

Compartir Me gusta Regístrate para ver qué les gusta a tus amigos.

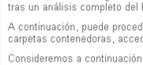
0 comentarios

Tags: defence intelligence, gdt, georgia tech information security center, anti malware, anti spyware, networkers community, bit, panda, fbi, webmaster

15 Mar 2010

## Gadgets INFEX + ActiveScan de Panda Security

Escrito por: [Carmen Martínez Ibáñez](#) el 15 Mar 2010 - [URL Permanente](#)



2 gadgets de utilidad para sus comprobaciones de seguridad en línea. [Pulse aquí \(\\*\)](#).

1. INFEX - The Malware Infection Index.

Índices estadísticos de infecciones por spyware en la red durante las últimas 24 h. con conexión a ActiveScan de Panda Security (Check + Project) para una examen completo de su PC.

2. NanoScan - Instant virus scan.

Análisis rápido de malware en su ordenador con indicaciones sobre el estado de su anti-virus (aplicaciones y actualizaciones) y recomendaciones a seguir.

Observaciones

Tal como comentamos en el informe sobre internet y seguridad, puede suprimir manualmente todo el malware, del modo siguiente según los resultados del siguiente informe de ejemplo exportado de ActiveScan tras un análisis completo del PC. [Pulse aquí.](#)

A continuación, puede proceder a suprimir los trackingcookie, spyware y virus, abriendo con su navegador las carpetas contenedoras, accediendo a las mismas, y eliminando los archivos infectados.

Consideremos a continuación tal como describe los resultados del examen, las ubicaciones o rutas de acceso. El modo de settings es abrir por ejemplo en el primer ítem de la lista propuesta, el directorio : c:\documents and settings\hp\_proprietario\cookies\

Situemos en la barra de direcciones de su navegador la ruta de acceso a la carpeta contenedora, una vez allí y tras abrir la ubicación, proceder a enviar el archivo a la papelera de reciclaje sin abrirlo: hp\_proprietario@doubleclick[1].txt

Posteriormente, deberá de esta manera completamente de su equipo todo rastro de malware vaciando la papelera de reciclaje, y operando de esta manera hasta suprimir todos los elementos infectados.

Compartir Me gusta Regístrate para ver qué les gusta a tus amigos.

0 comentarios

Tags: anti malware, anti spyware, panda

04 Mar 2010

## Defence Intelligence de Canadá detecta la botnet responsable de los ataques malware en la red

Escrito por: [José María Amenós Vidal](#) el 04 Mar 2010 - [URL Permanente](#)

Fuente : Globedia.

**Descubiertos los servidores remotos de origen desconocido que inyectaban código malicioso en sitios legítimos y disponían de la información de miles de usuarios.**

La denominada botnet (acrónimo de robot y red en inglés) fue detectada en mayo de 2009 por técnicos de la empresa canadiense Defence Intelligence, quienes crearon un grupo de trabajo para su seguimiento, junto a la empresa española Panda Security y el Georgia Tech Information Security Center. De manera paralela, la Oficina Federal de Investigaciones (FBI) inició una indagación sobre esa botnet y advirtió que un español estaba implicado, por lo que alertó a la Guardia Civil (\*).

La investigación se avoró en forma coordinada, lo que permitió conocer los vectores de infección de la botnet y sus canales de control de las computadoras ajenas. Asimismo, se determinó la existencia de un grupo de habla hispana, identificado como DOPTEAM, que había adquirido en el mercado del "malware" (programas maliciosos) el troyano utilizado.

La Guardia Civil explicó que una botnet es un conjunto de computadoras infectadas con un programa malicioso, que está bajo control de su administrador o "botmaster". Para su control, las computadoras infectadas, conocidas como bots, se conectan a un equipo llamado Command & Control (C&C) donde reciben instrucciones.

Las botnets pueden ser utilizadas para robar información de los propios equipos o para el uso clandestino de los mismos (envío de spam, atacar a terceros equipos o provocar denegaciones de servicio –DoS-).

**El botmaster puede usar esa información para sí o alquilarla a terceros, práctica muy habitual en bandas organizadas dedicadas al fraude bancario.**

Una de las botnets más grandes que se han detectado. En los registros efectuados en los domicilios de los detenidos fueron incautadas computadoras, material informático e información personal de más de 800 mil usuarios. "Los datos obtenidos por los ahora detenidos podían utilizarse para sí o alquilados a bandas organizadas dedicadas al fraude bancario".

**Dos prestadores de servicio americanos y uno español son los responsables directos de la infección de 13 millones de ordenadores.**

En diciembre pasado, tras identificar casi todos los canales de control de esa botnet, se procedió en forma coordinada a nivel internacional para bloquear los dominios que había utilizado. Estos se localizaban en especial en dos prestadores de servicio americanos y uno español.

La Guardia Civil española, en colaboración con la FBI y Panda Security, detuvo a tres españoles que controlaban más de 13 millones de computadoras infectadas, de las que obtenían datos personales y financieros.

**Técnicos canadienses de Defence Intelligence investigaron la denegación de servicio en miles de ordenadores en centros universitarios y administrativos de Canadá.**

Tras ese bloqueo, se produjo un importante ataque de denegación de servicio a la empresa Defence Intelligence, lo que afectó de manera seria a un gran Proveedor de Acceso a Internet (ISP).

Además, dejó sin conectividad durante varias horas a miles de clientes, entre los que figuraron centros universitarios y administrativos de Canadá.

Esa acción permitió conocer el resto de canales de control de la botnet, que al final fueron bloqueados ...

(\*) Grupo de Delitos Telemáticos (GDT) de la Guardia Civil y la Brigada de Investigación Tecnológica (BIT).

Compartir Me gusta Regístrate para ver qué les gusta a tus amigos.

0 comentarios

Tags: defence intelligence, gdt, georgia tech information security center, anti malware, anti spyware, networkers community, bit, panda, fbi, webmaster, globedia

16 Feb 2010

## IP - Internet Protocol

Escrito por: [Carmen Martínez Ibáñez](#) el 16 Feb 2010 - [URL Permanente](#)

En algunas ocasiones como webmaster nos podemos encontrar ante el dilema de bloquear o no con las herramientas de que disponemos por ejemplo en un CMS (Content Manager System), la dirección IP - Internet Protocol de un usuario por cuestiones de seguridad.

Esto ocurre cuando desde un proxy, host, PC, etc ... se establece múltiples conexiones y el comportamiento puede provocar consecuencias erráticas para nuestro servidor, por citar un caso concreto, a causa del envío masivo de correos electrónicos (spam).

Por esta razón, y para evitar esta situación, en los mencionados CMS como XOOPS 2.0, se dispone de un recurso de desconexión automática como mínimo durante 30 min. de las IPs que son origen de conflictos y que embrogan nuestra protección.

Sim embargo, y ante la reincidencia de estos comportamientos en ocasiones no existe otro medio práctico que bloquear de manera permanente la dirección que origina estos problemas, mayormente porque son origen y resultado de un programa informático que opera automáticamente enviando e-mails de forma indiscriminada.

Asimismo, con independencia de modificar el código genérico o específico. Hacemos en los ficheros del FTP - File Transfer Protocol y tras comprobar los motivos, como mencionamos en el ejemplo propuesto, envío masivo de correos electrónicos por spammers, podemos conocer información adicional sobre la IP monitorizada en el CMS y candidata a desconectar, antes de proceder a decidir su bloqueo definitivo.

LookUp IP.

Esta herramienta de consulta del protocolo de comunicación en una red está diseñada para proporcionar información adicional acerca de la dirección IP introducida.

Estos datos incluyen el nombre de host, la información de localización geográfica (incluye país, región, estado, ciudad, latitud y longitud y el código de área telefónica.) Y un mapa de ubicación específica. Los datos geográficos de referencia son extraídos de una base de datos de GPS - Global Positioning System.



La tecnología de geolocalización no es fiable al 100% en la prestación de ubicación puede estimarse en los casos óptimos sobre el 99%, aunque para las IPs en Estados Unidos, es del 90% a nivel estatal, y el 81% dentro de una zona de 25 millas. En general, y para todo el mundo la mínima precisión puede llegar a oscilar alrededor de un 60%.

Por ello, esta información no debe utilizarse para tratar de encontrar una dirección física exacta que requiera una precisión del 100%. Por favor, introduzca su dirección IP a buscar. [Pulse aquí.](#)

Blacklist Check

Esta opción que más nos interesa saber para decidir el bloqueo de la IP nos permite averiguar si la dirección de la que hemos buscado su información adicional, se encuentra en la lista negra de protocolos de Internet. [Pulse aquí.](#)

Compartir Me gusta Regístrate para ver qué les gusta a tus amigos.

0 comentarios

Tags: xoops, ip, gps

Leer siguientes Leer anteriores

## Networkers

Webmasters

15 Feb 2010

### PING Test

Escrito por: [José María Améndo Vidal](#) el 15 Feb 2010 - [URL Permanente](#)

Fuente : [SiteTimer OctaGate](#).

Ping Test comprueba el estado de conexión y es una herramienta para webmasters que se aplica para confirmar el funcionamiento de las páginas electrónicas, es decir, el comportamiento de los diferentes elementos que componen la página web cuando se carga en el navegador al abrir el sito en Internet.

Es una aplicación que se utiliza como refuerzo para hacer comprobaciones de seguridad que incluyen entre otros, la misma información que se obtiene de la directiva de privacidad de páginas web en Internet Explorer 8, o los detalles de malware y rendimiento de Google Labs.

¿Cómo funciona?

Cargas de ensayo de una página HTML completa, incluyendo todos los objetos (imágenes, CSS, JavaScripts, RSS, Flash y frames / frames, etc ...). Que imita la forma como una página se carga en un navegador web.

El tiempo de carga de todos los objetos se muestra visualmente con barras de tiempo.

Puede ver la lista de los objetos, ya sea en el orden de carga o como una jerarquía.

Cada prueba también muestra estadísticas generales sobre la página cargada, como el número total de objetos, el tiempo de carga total, y el tamaño incluyendo todos los objetos.

**Información del sitio web.**

Hemos seleccionado como ejemplo para su aplicación, el blog + CMS (Content Manager System) de estrategia info cuyos resultados se detallan en función de la siguiente información.

Tiempo de carga total: El tiempo total que tarda en cargarse la página incluyendo todos los objetos.

Total de objetos: El número total de objetos cargados que están relacionados con la página.

Los objetos externos: El número total de objetos de dominios externos.

- (X)HTML: Documentos HTML / XHTML, marcos e iframes.
- RSS/XML: Archivos y ficheros RSS y XML.
- CSS: Cascading Style Sheets.
- Scripts: JavaScripts externos.
- Imágenes: GIF, JPEG, PNG e ICO.
- Plugins: Archivos SWF de Flash.
- Otros: Tipo Indeterminado.
- Redireccionadas: Redirecciones a otras URL.

**Informes estadísticos**

Los informes estadísticos se pueden consultar en las siguientes urfs:

1. Blog - estrategia.info/pc. [Pulse aquí](#).
2. CMS - psicologos.estrategia.info. [Pulse aquí](#).

Las lecturas más importantes que interesan al webmaster son si todos los elementos cargados son los que se han autorizado y no existen por tanto intrusiones no autorizadas en el servidor remoto, lectura que también nos facilita la directiva de privacidad de páginas web en IEB.

Asimismo, comprobados los detalles de malware, se procede a leer el rendimiento del sitio, mediante la lectura del tiempo de carga promedio de todos los elementos, tal y como podemos comprobar en los detalles de malware y rendimiento de Google Labs.

El valor promedio de carga por elemento en el blog es de 2.3 seg. y en el CMS de 2.2 seg. lo cual significa que el tiempo de carga promedio para nuestro sitio es más rápido que el del 61-64 % de los sitios en la red ...

**Monitorización.**

La interpretación de los resultados que se desprende de la monitorización en los presentes informes estadísticos del blog y CMS, el tiempo promedio de carga actual es superior que en la toma de datos del 03/12/2009 a causa del tiempo de espera que tardan los lectores de feeds que dependen de dominios externos, en leer la información de los ficheros RSS/XML.

Compartir     

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 [Twitter](#) | 0

 0 comentarios

Tags: [pingdom](#)

12 Feb 2010

### Network Safety

Escrito por: [José María Améndo Vidal](#) el 12 Feb 2010 - [URL Permanente](#)

La seguridad de la red o trabajar con nuestro PC en un entorno seguro cuando nos conectamos a Internet son el motivo de este artículo.

Hemos podido comprobar que la implementación de varios programas antimalware y antispyware ofrecen un mínimo de garantías de desarrollar nuestras actividades minimizando al máximo el riesgo de ser blancos fáciles de los virus informáticos y software espía.

En la actualidad, y según las estadísticas más recientes, el 60 % de los PCs utilizados por los españoles se encuentran en un modo u otro infectados, el resto que solamente es del 40 % se ha visto obligado a utilizar estrategias seguras que permitan garantizar la protección efectiva de nuestros ordenadores.

Desde nuestra experiencia, podemos citar un ejemplo de entorno seguro con el único fin de no engrosar los altos índices citados a los que nuestro país se ha visto sometido, y que en definitiva, ronda el de los países con mayores valores de PCs infectados en el mundo.

Utilizaremos en nuestro caso práctico una plataforma Windows XP por tratarse de una aplicación muy generalizada hoy en día, que suele ir acompañada de Norton Internet Security + Anti-Virus, proveedor habitual cuando se adquiere un ordenador con software instalado de Microsoft.

A continuación, les recomendamos además de mantener actualizados los packs de dichas aplicaciones mediante la utilización con regularidad de Windows Update de Microsoft y LiveUpdate de Norton, la instrumentalización de los siguientes programas de seguridad y actualizaciones informáticas.

Asimismo, es recomendable realizar los exámenes de seguridad completos de nuestro PC con cada uno de los programas de seguridad señalados, con periodicidad semanal y tras actualizarlos.

**Firewall, antimalware y antispyware**

1. Microsoft Security Essentials, que es la última novedad en cuanto a protección en línea, creado y desarrollado para plataformas de Windows.
2. Windows Defender, un programa antispyware y firewall de uso básico para PC.

3. AVG Anti-Virus de Grisoft, una aplicación anti-malware con altas prestaciones de seguridad (opcional).
4. Panda USB Vaccine, que nos permite asegurar nuestra protección contra las infecciones que provienen de la inserción de dispositivos USB.

**Descargas y actualizaciones.**

5. Software Informer, que nos permite ser notificados sobre descargas disponibles de aquellos programas instalados en nuestro ordenador que necesitan para ser seguros de una versión más actualizada.
6. Free Download Manager, una aplicación que facilita la descarga segura de software en la red, y cuyo complemento "Remote Control Server" nos ayuda a proteger con contraseña el puerto 8080, cerrando este acceso que suele ser la puerta trasera de entrada para virus y troyanos.

**Exámenes de seguridad**

7. Malwarebytes Anti-Malware, especializado en detectar los archivos infectados con mayor dificultad de localización.
8. Windows Live OneCare, que tiene la particularidad de eliminar infecciones, corregir errores de código, reparar archivos desconfigurados, limpiar el sistema y desfragmentar el disco duro.

**Navegadores.**

9. Filtroado InPrivate de la publicidad, bloqueo de seguridad en Internet Explorer 8.

Compartir     

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 [Twitter](#) | 0

 0 comentarios

Tags: [anti malware](#), [anti spyware](#), [informer technologies](#), [networkers community](#), [norton](#), [microsoft](#), [windows](#), [usb](#), [panda](#), [webmaster](#)

06 Feb 2010

### Bloqueo de seguridad en IE8 : Filtroado InPrivate de la publicidad

Escrito por: [José María Améndo Vidal](#) el 06 Feb 2010 - [URL Permanente](#)



Fuente : [Microsoft](#).

1. Descargar fichero XML. [Pulse aquí](#).
2. En la pestaña de seguridad de su navegador Internet Explorer 8, marque en el menú la opción de "configuración de Filtroado InPrivate".
3. En la ventana que aparece pulse en "bloquear automáticamente" y a continuación en "configuración avanzada".
4. En el menú que visualiza de administración de complementos, debe marcar "Filtroado InPrivate" y ejecutar acto seguido la opción de "Importar" ...
5. Cargue ahora el fichero XML descargado anteriormente importando su contenido al administrador de complementos ...

A partir de este momento, cuando desee bloquear los anuncios publicitarios, solamente deberá marcar en la pestaña de seguridad de Internet Explorer 8 la opción del menú : Filtroado InPrivate.

Nota : El Filtroado InPrivate no está activado por defecto y de forma predeterminada en su navegador IEB.

Compartir     

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 [Twitter](#) | 0

 0 comentarios

Tags: [microsoft](#), [windows](#)

05 Feb 2010

### JAVA applet : Verificación de instalación + Prueba de máquina virtual

Escrito por: [Carmen Martínez Ibáñez](#) el 05 Feb 2010 - [URL Permanente](#)

Fuente : [Sun Microsystems](#).



La tecnología Java se utiliza en los equipos integrados de automóviles, aviones, coches e incluso en la sonda Mars Rover de la NASA.

Ofrece interactividad con internet, gráficos en tiempo real para televisión, imágenes al instante para cámaras digitales, y otras aplicaciones para teléfonos móviles y equipos multimedia.

Asegúrese de que tiene instalada la versión de Java recomendada para su sistema operativo. [Pulse aquí](#).

NOTA: si ha completado recientemente la instalación del software de Java, quizá deba reiniciar su navegador (cierra todas las ventanas del navegador y vuelve a abrirlas) antes de comprobar su instalación.

**Prueba de la máquina virtual de Java.**

**Plataformas:** Solaris, Linux, Windows ...

**Navegadores:** Internet Explorer, Firefox, Mozilla, Netscape ...

Versiones de Java: 1.4, 1.5, 6.0 ...

Para comprobar la configuración, el applet se muestra correctamente. [Pulse aquí](#).

Compartir     

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 [Twitter](#) | 0

 0 comentarios

Tags: [sun microsystems](#), [java](#)

29 Ene 2010

### AVG Anti-virus

Escrito por: [José María Améndo Vidal](#) el 29 Ene 2010 - [URL Permanente](#)

Aunque en situaciones excepcionales de ataques malware debería ser suficiente que el anti-virus funcione sin más novedad que eliminar el software espía o virus informático que afecta nuestro ordenador, nos hemos encontrado con la necesidad de aplicar los productos de AVG Technologies para proteger nuestros PCs, situando en su bóveda de virus los archivos a reparar.

Por esta razón, recomendamos que en casos de extrema gravedad, recurran puntualmente a la utilización de este programa de seguridad, a pesar de tener instalado en su ordenador anti-virus de otros proveedores.

En ocasiones puede ocurrir que los cada vez más sofisticados medios de que dispone el malware para instalarse en su PC, hagan de su tarea por combatirlo con los recursos habituales, un medio ineficaz que no logra impedir su intrusión, haciendo prácticamente imposible detener la infección. Sin embargo, con la ayuda del Anti-virus de Grisoft y por experiencia, sabemos que ha sido posible eliminar la amenaza.

En el ejemplo que mencionamos, decidimos instalar esporádicamente y de una forma puntual esta aplicación aunque utilizamos habitualmente otros productos, fue a causa de un bloqueo por malware de las necesarias actualizaciones automáticas de nuestro anti-virus, lo cual provocó que se inhabilitara su actualización periódica, haciendo que nuestro ordenador quedara desprotegido, y expuesto a merced de cualquier software malintencionado de última generación.

Pudimos comprobar de esto modo y una vez solucionada la incidencia que se hizo indispensable utilizarlo excepcionales. Dejo de registrar habitual sistema de protección con el fin de solucionar problemas que puedan resultar ser potencialmente peligrosos.

AVG Anti-virus es una opción de calidad en su decisión de elegir entre los mejores programas de seguridad informática.



**Anti-Virus de Grisoft**

Fuente : [AVG Technologies](#).

**Protección antivirus para satisfacer sus necesidades básicas de seguridad.**

El nombre corporativo de Grisoft ha cambiado a AVG Technologies, pero desde siempre su filosofía ha sido que todos tienen derecho a la seguridad básica del equipo de forma gratuita.

Son 110 millones de usuarios los que utilizan sus productos de seguridad. De manera que si planea permanecer en línea e intercambiar archivos es una buena opción.

Navegue y realice búsquedas con confianza, mientras LinkScanner lo protege de sitios nocivos.

Obtenga protección en línea y fuera de línea contra virus, spyware y otras sorpresas desagradables.

Disfrute de un rendimiento uniforme y de alta velocidad del equipo con el nuevo analizador de virus mejorado.

Las actualizaciones automáticas mantienen la **protección básica anti-virus y anti-spyware para Windows disponible mediante descarga gratuita**. [Pulse aquí](#).

Compartir     

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 [Twitter](#) | 0

 0 comentarios

Tags: [avg technologies](#), [anti malware](#), [anti spyware](#), [windows](#)

25 Ene 2010

### Software Informer

Escrito por: [José María Améndo Vidal](#) el 25 Ene 2010 - [URL Permanente](#)

Fuente : [Software Informer](#).

No siempre es suficiente saber que un programa, instalado en su PC, ha funcionado hasta ahora a prueba de fallos.

A pesar de que usted puede utilizar su software solamente para un conjunto definido de funciones, alguna vez puede ocurrir que algunos datos específicos o un sutil cambio en la configuración general produzca un conflicto que desconoce. El resultado puede ser un error de software que es preocupante, pero puede ser prevenido.

Software Informer es un programa que ha sido especialmente diseñado para aquellos usuarios que se preocupan de mantener sus aplicaciones funcionales listas para cualquier tarea que pueda surgir.

Su objetivo principal es darle una información general y específica de las descargas disponibles y actualizadas sobre el software que realmente utiliza.

Para ello, este programa hará una lista de aplicaciones instaladas en su ordenador y, posteriormente, realizará comprobaciones periódicas de las versiones y se lo comunicará de vez en cuando mediante una conexión a un servidor de expansión con una actualización constante de su lista de aplicaciones. Siempre le indicará una versión más reciente de cualquiera de los programas de que disponga, es decir, le notificará y ofrecerá un enlace para descargar la actualización. [Pulse aquí](#).

Pero este programa va más allá. Le proporcionará una interfaz centralizada durante todo el proceso con el fin de obtener información pertinente sobre todas las herramientas que puedan interesarle. Lo que le permite hacer un seguimiento de las observaciones y preguntas sobre el software correspondiente.

Compartir     

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 [Twitter](#) | 0

 0 comentarios

Tags: [informer technologies](#)

23 Ene 2010

### Secunia PSI

Escrito por: [Carmen Martínez Ibáñez](#) el 23 Ene 2010 - [URL Permanente](#)



Fuente : [Personal Software Inspector](#).

El usuario medio, sin Secunia PSI cuenta con 12 programas inseguros instalados en su PC.

¿ Vulnerable ?

¿Sabía usted que muchos de los ataques de hackers y amenazas a la seguridad aprovechan en la actualidad las vulnerabilidades de programas y errores de código?.

¿Conoce los programas que tiene instalados y que estos le pueden exponer a amenazas de seguridad?.

¿ Seguro ?

¿ Su PC está seguro? ¿Tiene todas las últimas actualizaciones y los parches de seguridad al día?.

¡ Protejase !

Las revisiones de seguridad son generalmente libres y disponibles para descargar desde el programa de los proveedores. Dejo que Secunia PSI determine exactamente las actualizaciones y parches que necesita para proteger su PC.

Secunia PSI - Personal Software Inspector es una herramienta de seguridad gratuita diseñada con el único propósito de ayudarle a proteger el equipo contra las vulnerabilidades en sus programas. [Pulse aquí](#).

Compartir     

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 [Twitter](#) | 0

 0 comentarios

Tags: [secunia](#)

15 Ene 2010

### Offline Explorer

Escrito por: [José María Améndo Vidal](#) el 15 Ene 2010 - [URL Permanente](#)

Aunque es poco habitual pero igualmente efectivo, hoy hablamos de realizar copias de seguridad de tus webs mediante la utilización del programa Offline Explorer. [Pulse aquí](#).

Estamos acostumbrados a realizar el backup de datos de nuestras páginas electrónicas o utilizar por ejemplo programas como es Xampp - Apache, FTP, MySQL (\*) para la implementación de un host local, ... lo cual convierte estas herramientas del webmaster en maniobras básicas para el mantenimiento y gestión de nuevos sitios en la red.

No obstante, con Offline Explorer podemos conseguir capturar un espacio completo en Internet, con el fin de conservar en un CD o soporte informático portable, todas las características de una página electrónica, y por la que incluso, se puede navegar sin conectarnos a Internet, de modo que también nos permita, trabajar sin conexión, o mantener en su integridad todos sus archivos ejecutables.

Este modo de realización de una copia de seguridad, nos puede ser de utilidad por ejemplo en caso de trasladar de servidor DNS o de registrar nuestra dirección electrónica, cargando en el host del nuevo proveedor de Internet de nuestra dirección electrónica, el espacio web que copiamos con Offline Explorer del antiguo servidor remoto.

Sin más, les facilitamos un link en el cual pueden comprobar la calidad de ejecución de este programa, que nos permite importar y/o exportar todas las prestaciones de un espacio web. [Pulse aquí](#).

(\*) Para más información sobre Xampp - Apache, FTP, MySQL ... puede consultar este apartado en nuestro informe sobre Internet y Seguridad.

Compartir     

 Me gusta  Regístrate para ver qué les gusta a tus amigos.

 [Twitter](#) | 0

 0 comentarios

Tags: [metaproducts](#), [webmaster](#)

07 Ene 2010

### Windows Defender

Escrito por: [Carmen Martínez Ibáñez](#) el 07 Ene 2010 - [URL Permanente](#)

10 Dic 2009

## Anti-virus para dispositivos USB

Escrito por: [José María Amenós Vidal](#) el 10 Dic 2009 - [URL Permanente](#)Fuente : **Antimalware Panda USB Vaccine.**

Solución gratuita antimalware que se propaga a través de unidades USB. Cada vez son más los ejemplares de malware, entre ellos el peligroso Conficker, que se propaga mediante la infección de dispositivos y unidades extraíbles como llaves de memoria, reproductores MP3, cámaras de fotos, etc ... Para ello, estos códigos maliciosos realizan una modificación del fichero Autorun, presente en esas unidades.



**Panda USB Vaccine** es una **solución gratuita antimalware** diseñada para proteger contra este creciente peligro. Para ello, permite llevar a cabo una **doble protección preventiva, o vacuna, tanto del mismo PC para deshabilitar la funcionalidad AutoRun, como de unidades y llaves USB individuales.**

**Vacuna de equipos** : permite "vacunar" sus equipos para impedir que ningún archivo Autorun se ejecute independientemente de si el dispositivo en el que se encuentra (llave de memoria, CD, etc.) está infectado o no.

**Vacuna de dispositivos USB** : permite "vacunar" dispositivos extraíbles USB de manera individual, de tal modo que ningún archivo Autorun incluido en los mismos pueda ser una fuente de infección, ya que la herramienta los deshabilita, evitando así que puedan ser leídos, creados, modificados o suprimidos por un código malicioso.

Se trata de una herramienta muy útil, ya que no existe una manera sencilla de deshabilitar la opción de Autorun en Windows. Con esta herramienta, los usuarios podrán hacerlo de manera sencilla, logrando así un alto grado de seguridad respecto a las infecciones procedentes de dispositivos extraíbles.

Puede descargar gratuitamente antimalware **Panda USB Vaccine**. [Pulse aquí.](#)

Compartir

Me gusta Regístrate para ver qué les gusta a tus amigos.

[Twitter](#) 0

0 comentarios

Tags: [anti malware](#), [usb](#), [panda](#)

07 Dic 2009

## Internet y Seguridad

Escrito por: [Carmen Martínez Ibáñez](#) el 07 Dic 2009 - [URL Permanente](#)

### WAM - Web Anti-Malware.

#### Sumario.

Introducción. 1. Análisis, detección y eliminación de Malware. 2. Protección con contraseña del puerto 8080, actualizar a IEB e implementar un host local. 3. Cambiar la clave de acceso FTP y modificar el archivo .htaccess. Conclusiones. Google Search y Dasient WAM - Web Anti-Malware. Apéndice. Notas y Textos. Referencias bibliográficas. Agradecimientos. Palabras Clave.

#### Resumen.

#### Introducción.

El malware es todo tipo de software espía, virus informáticos, etc ... que se intenta insertar a través de iframes, scripts ... en el código fuente de las páginas web sin conocimiento del webmaster para infectar los PCs de los usuarios.

#### 1. Análisis, detección y eliminación de Malware.

La implantación de un rastreador anti-malware en su PC, es decir, del programa Malwarebytes Anti-Malware para análisis y reparación de código malicioso, ... junto a la intervención del examen de Windows Live OneCare (y también de Microsoft Security Essentials) ...

#### 2. Protección con contraseña del puerto 8080, actualizar a IEB e implementar un host local.

La protección con contraseña del puerto 8080, con la aplicación de FDM Remote Control Server de Free Download Manager, ... y la actualización a Internet Explorer 8 con la utilización simultánea de la directiva de privacidad de páginas web ...

El uso del programa de simulación XAMPP : Apache, FTP, MySQL ... para ayudar a recuperar la página electrónica original y hacer efectiva su actualización (por ejemplo a XOOPS 2.0.) con el fin de mejorar su seguridad, ...

#### 3. Cambiar la clave de acceso FTP y modificar el archivo .htaccess.

El cambio en la clave de acceso FTP - File Transfer Protocol y la modificación de archivos en los que se ha introducido código específico y genérico .htaccess contra la infección en nuestro servidor.

#### Conclusiones.

Y la instrumentalización de las herramientas del webmaster de Google así como del programa de prevención de intrusiones Dasient WAM, ...

Hacen de todas estas medidas adoptadas a día de hoy una metodología efectiva para garantizar la seguridad en la web, como si nuestro sitio en la red se tratara de un banco nacional, ...

La regla de oro de la seguridad en Internet es mantener actualizados tanto los anti-virus como las aplicaciones informáticas de nuestro PC.

Un ejemplo de programa que también nos servirá para complementar la protección de nuestros ordenadores es Microsoft Security Essentials.

#### Notas.

En realidad, los tres pasos fundamentales primera y anteriormente citados son los más importantes, para proteger a los usuarios y su sitio legítimo de posibles infecciones a causa de la inserción de código malicioso sin su conocimiento ... el complemento del archivo .htaccess es para fortalecer su protección ante nuevos ataques de malware.

En definitiva, si a pesar de todo existe aviso en el buscador Google de que su sitio ha distribuido durante los últimos 90 días software malicioso por causas ajenas a su voluntad, ... deberán utilizar las herramientas del webmaster, y seguir las instrucciones para introducir un código "meta" entre las etiquetas "head" antes de "body" de su web, ... para verificar que Ud. es el propietario del sitio en la red, ...

Y posteriormente utilizar el formulario habilitado al efecto y dirigir un correo al staff de Google search para que vuelvan a comprobar su sitio ya limpio de malware para conseguir eliminar el aviso de sitio malicioso.

#### Agradecimientos.

La elaboración del presente artículo es el resultado del trabajo realizado en estrategia.info del 25 de junio al 3 de septiembre de 2009, y ha sido posible gracias a la colaboración de Antonio Amenós Vidal - e-mail : soporte@estrategia.info, webmaster de Networkers Community ...

Continuación ...

Compartir

Me gusta Regístrate para ver qué les gusta a tus amigos.

[Twitter](#) 0

1 comentario

Tags: [anti malware](#), [networkers community](#), [webmaster](#)

[Leer siguientes »](#)