Como bloquear los Bad bots (Bot basura) usando ModeSecurity en Directadmin v1

Introducción BadBots

El término "bot" se utiliza frecuentemente en internet y se refiere a un programa informático que automatiza acciones o tareas en la red. Aunque un bot no es inherentemente bueno o malo, puede clasificarse en alguna de estas dos categorías, dependiendo de si se utiliza con buenas o malas intenciones.

Bots Buenos

Se llama "bot bueno" a aquel que realiza tareas útiles o beneficiosas que no perjudican la experiencia del usuario en internet. Hay muchos bots que se consideran buenos, por ejemplo:

- Bots de Motores de Búsqueda: A menudo conocidos como rastreadores web o arañas, son operados por grandes motores de búsqueda como Google o Bing.
- Bots de Monitoreo de Sitios: Estos bots supervisan métricas de páginas web, como el seguimiento de enlaces o caídas del sistema, y pueden alertar a los usuarios sobre cambios importantes o tiempos de inactividad. Son utilizados por sitios como UptimeRobot o Cloudflare.
- Bots de Feed: Estos bots recorren internet en busca de contenido para añadir a los feeds de noticias de diversas plataformas, y son gestionados por sitios de agregación o redes sociales.
- Bots de Asistentes Personales: Aunque estos programas son más avanzados que un bot típico, siguen siendo considerados bots. Son programas informáticos que buscan datos en internet que coincidan con una búsqueda, y son operados por empresas como Apple (Siri) o Google (Alexa).

Bots Malos

Por otro lado, se refiere como "bot malo" a aquellos que realizan actos maliciosos, roban datos o causan daños en servidores, redes o sitios web. Pueden ser empleados para llevar a cabo ataques de denegación de servicio distribuido (DDoS) o para escanear servidores, redes o páginas web en busca de vulnerabilidades que puedan comprometer estos sistemas.

En los últimos años, hemos visto que los bots maliciosos se han convertido en un problema significativo tanto para los administradores de servidores como para los dueños de sitios web. Estos bots suelen dirigirse a un servidor o página web, realizando miles de solicitudes y recopilando grandes cantidades de datos en un tiempo muy corto.

Su practica, su diseño, y su falta de ética son un problema para muchos sitos, sus administradores y los administradores de sistemas.

Técnicas de bloqueo

Hay algunas técnicas de bloqueo como el uso de .htaccess a través de formulas como la expuesta en Bad Bots y la pesadilla del tráfico. Htaccess en Apache 2.4:

```
# Start Bad Bot Prevention
<IfModule mod_setenvif.c>
# SetEnvIfNoCase User-Agent ^$ bad_bot
SetEnvIfNoCase User-Agent "^12soso.*" bad_bot
SetEnvIfNoCase User-Agent "^192.comAgent.*" bad_bot
SetEnvIfNoCase User-Agent "^1Noonbot.*" bad_bot
...
<Limit GET POST PUT>
  Order Allow,Deny
  Allow from all
  Deny from env=bad_bot
</Limit>
</IfModule>
```

Pero esto es una pesadilla a nivel administrador de sistemas, donde cada uno pone su lista.

Para mi, la mejor es el uso de ModSecurity y como ya me dedico prioritáriamente a Directadmin lo dejaré aquí más claro.

Bad Bots bloqueados en Directadmin con ModSecurity

Para usar este método tenemos que hacerlo de manera que no se sobre escriba la configuración cuando se actualiza Directadmin, Apache o Nginx

Crear el directorio si no existe

```
cd /usr/local/directadmin/custombuild
mkdir -p custom/modsecurity/conf
```

Crear 00_bad_bots_conf

```
nano /usr/local/directadmin/custombuild/custom/modsecurity/conf/00_bad_bots.conf
```

Contenido

```
# BLOCK BAD BOTS
SecRule REQUEST_HEADERS:User-Agent "@pmFromFile bad_bot_list.txt"
"phase:2,t:none,t:lowercase,log,deny,severity:2,status:406,id:1100000,msg:'Custom WAF Rules:
WEB CRAWLER/BAD BOT'"
```

> Atención a la rule ID, para que no choque con otra rules si tenias con anterioridad alguna adicional en otro sistema, o tienes un sistema para controlar las rules tuyas. Aquí usaremos `1100000`

Crear bad_bot_list.txt

Esta lista puedes actualizarla con la lista Apache Ultimate Bad Bot

El fichero a usar es `https://raw.githubusercontent.com/mitchellkrogza/apache-ultimate-bad-bot-blocker/master/_generator_lists/bad-user-agents-htaccess.list`

```
wget -O /usr/local/directadmin/custombuild/custom/modsecurity/conf/bad_bot_list.txt
https://raw.githubusercontent.com/mitchellkrogza/apache-ultimate-bad-bot-
blocker/master/_generator_lists/bad-user-agents-htaccess.list
```

O con curl

```
curl -o /usr/local/directadmin/custombuild/custom/modsecurity/conf/bad_bot_list.txt
https://raw.githubusercontent.com/mitchellkrogza/apache-ultimate-bad-bot-
blocker/master/_generator_lists/bad-user-agents-htaccess.list
```

También puedes crear una estrategia, para usando dicha lista eliminar o añadir los tuyos propios, cuando se actualice.

Actualización

```
da build modsecurity_rules
da build rewrite_confs
```

Verificación

Puedes verificar que esta correcto con el siguiente comando, que te mostrará que lo usado se copio en el lugar apropiado.

```
ls -la /etc/modsecurity.d/*bad*
-rw-r--r-- 1 root root  199 Jan  4 09:24 /etc/modsecurity.d/00_bad_bots.conf
-rw-r--r-- 1 root root 5534 Jan  4 09:26 /etc/modsecurity.d/bad_bot_list.txt
```

Testing

```
curl -A "AiHitBot" https://example.com
  <html>
  <head><title>406 Not Acceptable</title></head>
  <body>
  <center><h1>406 Not Acceptable</h1></center>
  <hr><center>nginx</center>
  </body>
  </html>

curl -A "aihitbot" https://example.com
  <html>
  <head><title>406 Not Acceptable</title></head>
  <body>
  <center><h1>406 Not Acceptable</h1></center>
  <hr><center>nginx</center>
  </body>
  </html>
```

> Reemplaza example.com con un dominio del servidor □□

Deberas obtener un **406 Not Acceptable** como respuesta

Agradecimientos

- How to Block Bad Bots using ModSecurity with DirectAdmin

Aviso

Esta documentación y su contenido, no implica que funcione en tu caso o determinados casos. También implica que tienes conocimientos sobre lo que trata, y que en cualquier caso tienes copias de seguridad. El contenido el contenido se entrega, tal y como está, sin que ello implique ningún obligación ni responsabilidad por parte de Castris

Si necesitas soporte profesional puedes contratar con Castris soporte profesional.

Revision #3
Created 2025-01-04 10:35:49 UTC by Abkrim
Updated 2026-02-01 08:33:56 UTC by Abkrim