Comprobamos que no haya ningún cron corriendo:

```
crontab -l
```

Comprobamos que no sea ninguna query lenta:

```
mysql -uadmin -p`cat /etc/psa/.psa.shadow`
show proccesslist;
show full processlist;
```

Comprobamos las conexiones:

```
netstat -putan
```

Comprobamos numero de accesos por IP en los logs de apache de cada dominio:

```
awk '{print $1}' /var/www/vhosts/*/logs/access_log | sort | uniq -c | sort -
n
```

Comprobamos el número de IP distintas que acceden al servidor:

```
cat access_log.processed | cut -d " " -f 1 | sort | uniq | wc -l
```

Si encontramos algún patrón de IP pero desconocemos sobre que dominio se está acometiendo el ataque comprobamos con server-status: Reinicamos apache:

```
systemctl restart httpd.service
```

Vamos a un navegador: http://86.109.107.216/server-status

Una vez tengamos el dominio, buscamos el log correspondiente filtrando por la IP sospechosa:

```
grep "dd/Mmm/aaaa:hh:mm" /var/www/vhosts/dominio.tld/logs/error_log | grep
IP.IP.IP.IP | ccza -A
```

Si estamos seguros de que se trata de un atacante o un bot maligno, bloqueamos en el firewall

Herramienta para ir monitorizando los procesos y recursos:

```
htop
```

From:
https://wiki.merkatu.info/ - **Wiki de merkatu**

Permanent link:
https://wiki.merkatu.info/procedimiento_ante_ataques?rev=1481791666

Last update: **2017/03/27 17:43**