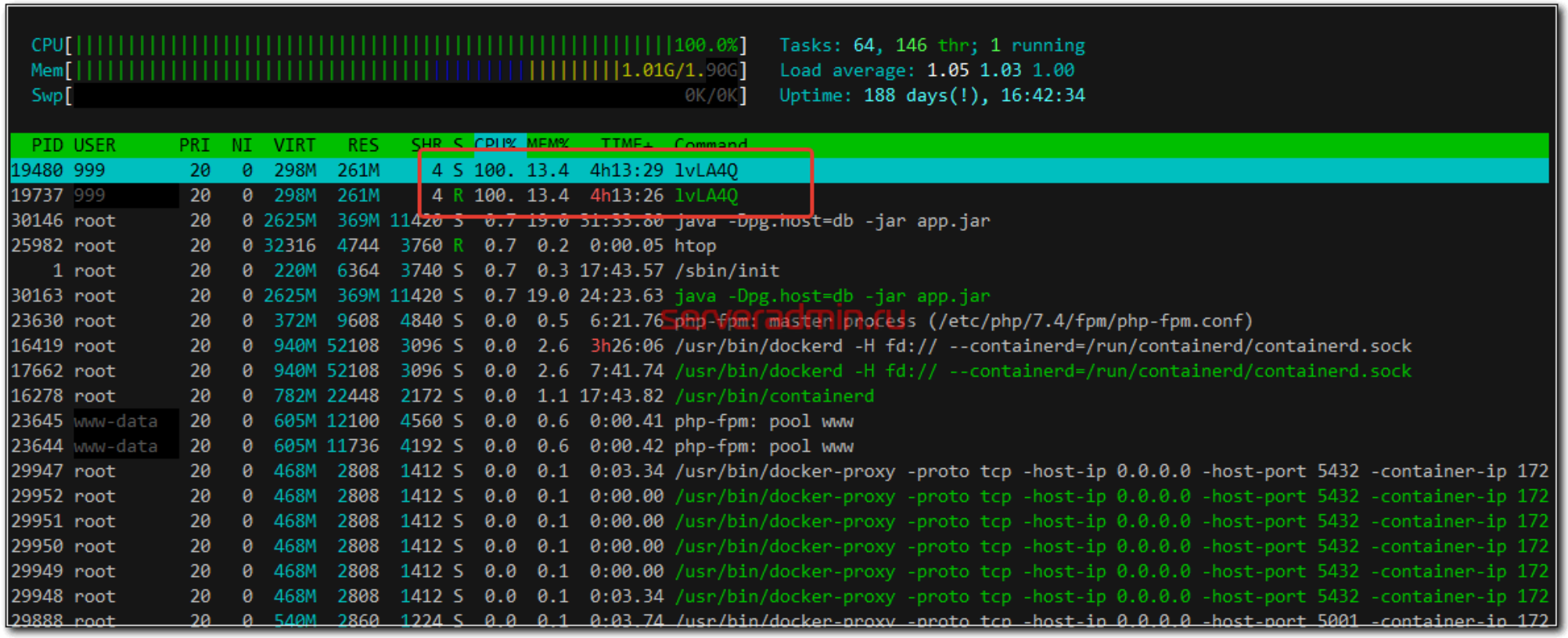
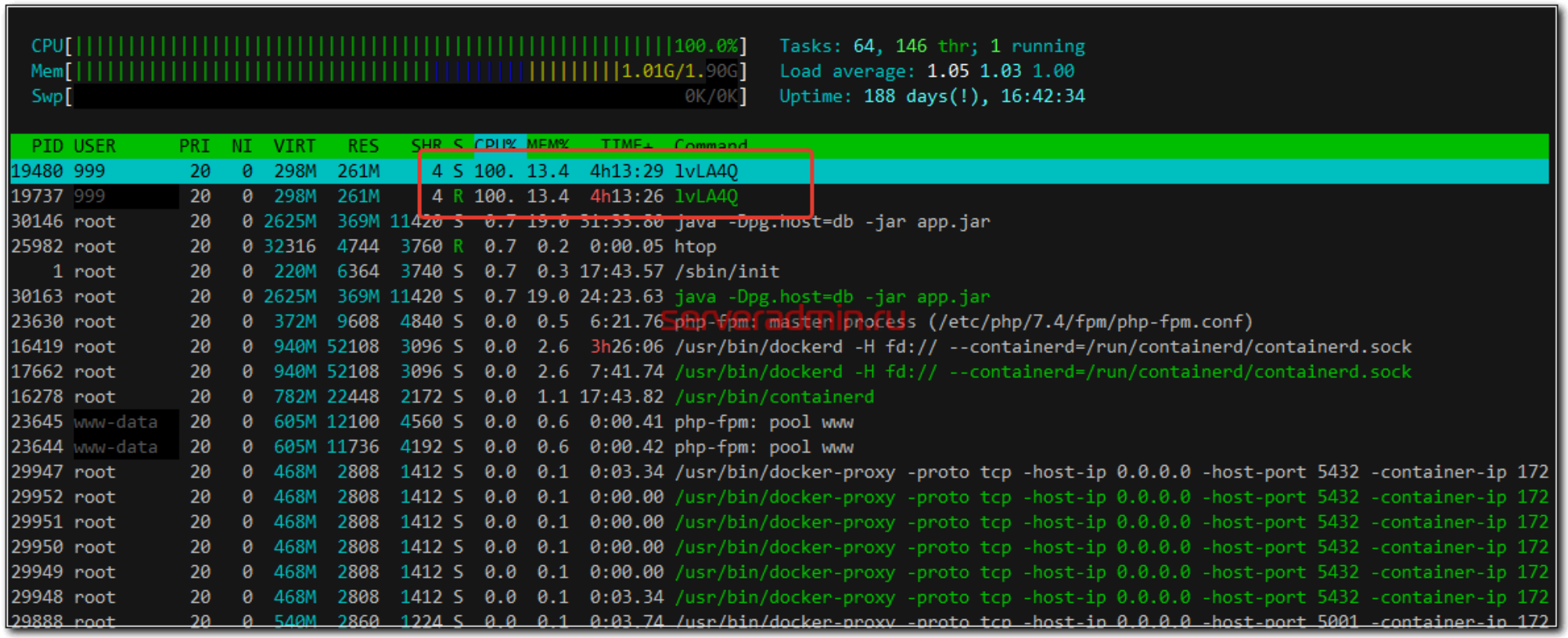


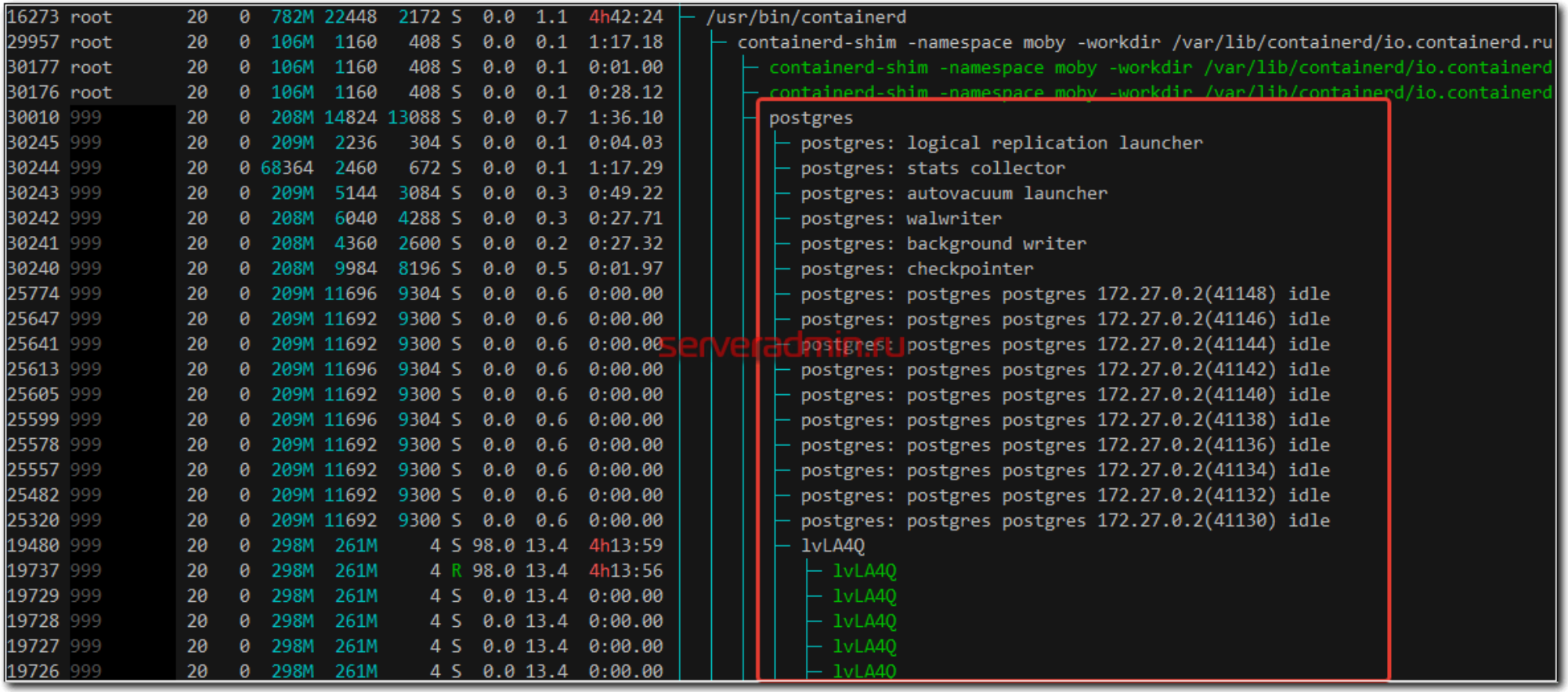
Небольшой пример из практики на тему того, как ломают web сервера на Linux. А то некоторые думают, что под линуксом вирусов нет, или что Linux настолько безопасен, что его даже защищать не надо. В общем, показательная история из жизни. Ничего особенного, просто пример, которых наверняка много у любого админа, который работает с разработчиками.

регистрации.

Пересылает мне утром владелец учетной записи в Hetzner информацию о том, что пришло уведомление, что у нас на одном из серверов подозрительная активность и его вырубят, если мы ничего не сделаем. Это тестовый сервер разработчика. Иду по ssh на сервер и вижу.



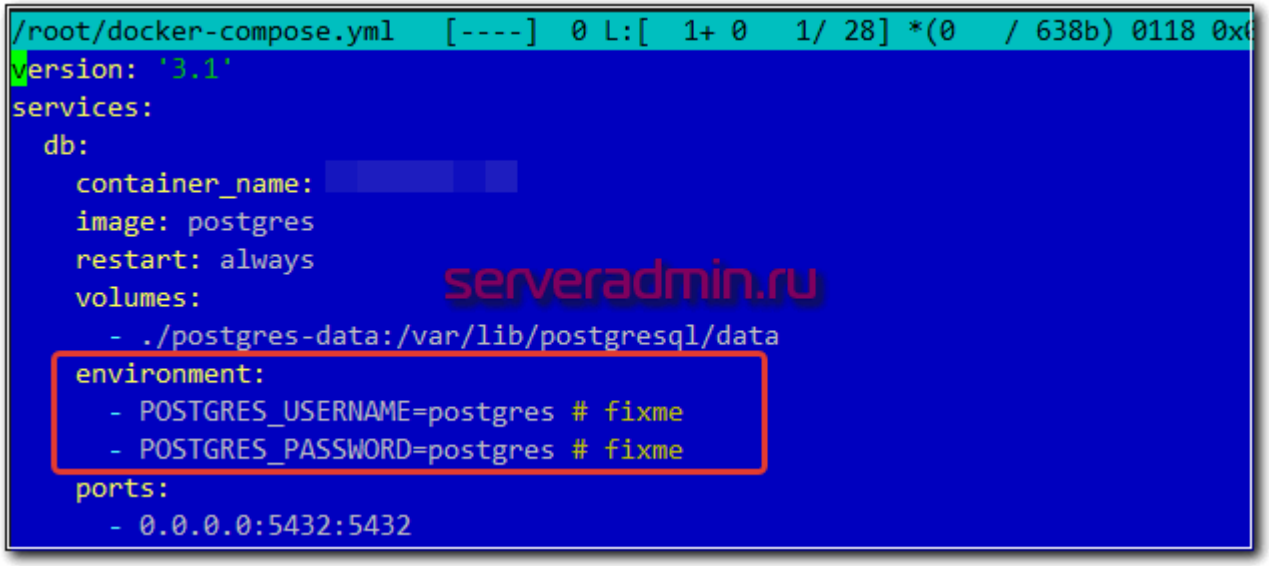
Вижу явный вирус. Думаю, что майнер какой-нибудь (на виртуалке за 3 евро, хе-хе). Смотрю дерево процессов, чтобы понять, откуда ноги растут.



Все понятно. На сервере стоит Docker. В нем контейнер Postgres. Вирус сидит в контейнере. Иду смотреть, как запущен контейнер. Ничуть не удивлен тем, что он смотрит напрямую в инет.

```
root@r      :~# netstat -tulnp
Active Internet connections (only servers)
Proto Recv-Q Send-Q Local Address           Foreign Address         State       PID/Program name
tcp        0      0 0.0.0.0:443             0.0.0.0:*               LISTEN      13616/nginx: master
tcp        0      0 0.0.0.0:80              0.0.0.0:*               LISTEN      13616/nginx: master
tcp        0      0 127.0.0.53:53           0.0.0.0:*               LISTEN      775/systemd-resolve
tcp        0      0 0.0.0.0:22              0.0.0.0:*               LISTEN      1024/sshd
tcp6       0      0 :::5001                 :::*                    LISTEN      29888/docker-proxy
tcp6       0      0 :::22                   :::*                    LISTEN      1024/sshd
tcp6       0      0 :::3000                 :::*                    LISTEN      6083/docker-proxy
tcp6       0      0 :::5432                 :::*                    LISTEN      29947/docker-proxy
udp        0      0 127.0.0.53:53           0.0.0.0:*                           775/systemd-resolve
udp        0      0 0.0.0.0:68              0.0.0.0:*                           763/dhclient
root@r      :~#
```


Дальше решил проверить, с какими параметрами он запущен. Опять не удивляюсь.



В лучших традициях жанра, все запущено с дефолтной учеткой postgres/postgres. Фраза fixme игнорируется.

Решил на всякий случай проверить прод. **Захожу, а там все то же самое**, но вируса пока нет. Не стал разбираться, чтобы ненароком не словить бан от Hetzner. Первую виртуалку просто удалили. На второй сразу поменяли пароль.

Вот так легко и просто взламываются веб сервера под Linux. Ожидали чего-то большего? Не нужны никакие хакеры, суперсофт и скилл. Достаточно взять какой-то сканер и найти открытые в инет службы. Затем проверить дефолтные пароли к ним и наверняка что-то подойдет. Разработчиков с каждым годом все больше и больше, докер контейнеров тоже. Так что ломать сервера будет все проще и проще.

Тут, конечно, есть недоработка докера. Он зачем-то по дефолту мапит контейнеры к 0.0.0.0, а не к локалхосту. Понятно, что так проще разработчикам, но результат налицо. Разработчики чаще всего не парятся над этим и даже не обращают внимание. Я постоянно вижу на dev серверах контейнеры с backend, смотрящие напрямую в инет. Так что надо обязательно вручную заблокировать доступ к контейнерам Docker из интернета.

В данном случае, достаточно было заблокировать доступ к postgres с помощью iptables:

```
/sbin/iptables -I DOCKER-USER -i eth0 -p tcp --dport 5432 -j DROP
```

> Не понравилась статья и хочешь научить меня администрировать? Пожалуйста, я люблю учиться. Комментарии в твоем распоряжении. Расскажи, как сделать правильно!

Расскажите, встречались с похожими, простыми и очевидными факапами?

Помогла статья? Подписывайся на telegram канал автора

Анонсы всех статей, плюс много другой полезной и интересной информации, которая не попадает на сайт.