Шкідливі скрипти на сервері

Рано чи пізно цей день настане, то ж підготуватись не завадить. Отож перше що потрібно зробити - це банально встановити антивірус.

Clamav - антивірус

Встановлюємо

```
# apt-get install clamav
```

Команда для одноразової перевірки

```
clamscan -i -r  --max-dir-recursion 500 --move /home/virus/Infected/ --
log=/home/user/clam.log /var/www/
```

Зверніть увагу також буде перевірено карантин, щоб
уникнути цього - перенесіть карантин в інше місце

Розберемо деякі аргументи

- max-dir-recursion - глибина вкладення каталогів, можна вказати менше
- move - вказівка переносити заражені файли в каталог (в даному випадку /home/virus/Infected/ - зверніть увагу каталог повинен існувати)
- log=/var/log/clamav.log - вказівка записувати дії в файл (бажано налаштувати також ротацію логів)
- /var/www/ - що саме перевіряємо, може відрізнятись

Якщо у вас сайти в домашній директорії користувачів (і це правильно!) команда буде мати вигляд

```
clamscan  -i  -r --max-dir-recursion 500 --remove --log=/home/user/clam.log
/home/
```

Clamav - безкоштовний та досить простий антивірус, детальніше про його налаштування на окремій сторінці - тут лише загальна команда, яку варто внести в Cron

Приклади шкідливих файлів, що трапились мені останнього разу

```
AbstractCliApplication.php Encapsulation.php ajax.php ajax23.php ajax30.php
ajax61.php ajax92.php article.php article22.php article80.php article94.php
banner.php behavior.php blog.php blog27.php cache.php cache27.php
cache52.php code.php code36.php code45.php code71.php css.php css72.php
css73.php default.php diff.php diff55.php diff75.php diff76.php dir.php
dirs.php dirs13.php dirs45.php dump.php dump66.php error.php error78.php
```

```
file36.php file42.php files.php files74.php files9.php footer.php
footer11.php footer7.php footer97.php functions26.php functions29.php
functions8.php gallery.php gallery18.php gallery50.php general26.php
general91.php global.php global26.php global4.php help.php help67.php
help69.php help93.php helper.php image.php inc.php inc48.php inc98.php
include24.php info.php info55.php info61.php info84.php ini.php ini21.php
ini29.php ini86.php ini99.php installscript.php javascript.php languages.php
lib.php list.php list33.php list40.php list82.php list94.php log.txt
menu.php model62.php object.php object55.php object83.php page.php
page76.php plugin.php plugin92.php press.php press92.php proxy.php
proxy16.php proxy53.php router.php session.php session63.php sql.php
start.php start20.php start66.php start87.php stats.php stats66.php
stats87.php system.php system3.php system87.php template49.php
template73.php test.php test8.php test88.php themes.php themes8.php
themes92.php title.php title33.php title67.php title9.php user.php utf.php
utf92.php view.php view52.php xml.php xml31.php xml7.php yrvepqbm.php
```

Неофіційні бази Clamav

Якщо з основними базами є почуття непевності то можна встановити неофіційні бази - робиться це доволі просто

```
# apt-get install clamav-unofficial-sigs
```

Далі все стандартно

Свої бази Clamav

Clamav дає змогу самостійно наповнювати базу, для цього є утиліта sigtool

Для початку дізнаємось її розташування

```
whereis sigtool
```

В Xubuntu вона є за адресою

```
/usr/bin/sigtool
```

Далі використовуємо таку конструкцію

```
cat ./patch/virus.php | /usr/bin/sigtool --hex-dump | head -c 2048 >>
./patch/clamav_bases/djsigs.ndb
```

Пояснення - тут ми передаємо вірусний файл, що лежить за шляхом ./patch/virus.php на утиліту, та формуємо сигнатуру. Після цього пишемо її у файл djsigs.ndb

Щоб цей файл запрацював додамо перед самою сигнатурою

```
{HEX}base64.first.malware:0:*:
```

Повинно вийти щось, схоже на це

Тепер потрібно скопіювати цей файл в теку з базами

Зазвичай це

```
/var/lib/clamav/
```

Готово - тепер можна просканувати усю теку й дізнатись де ще є цей же вірус.

Maldet

Ще одне рішення для видалення зарази з серверів, цього набору скриптів в репозиторіях немає - тому спочатку потрібного його завантажити

Йдемо в потрібну директорію й завантажуємо туди архів

```
# cd /usr/local/src && wget
http://www.rfxn.com/downloads/maldetect-current.tar.gz
```

або можна в домашню

```
# cd ~ && wget http://www.rfxn.com/downloads/maldetect-current.tar.gz
```

Розпаковуємо

```
# tar -xzvf maldetect-current.tar.gz
```

переглядаємо що у нас є

```
# ls
```

Бачимо папку maldetect-* - де зірочка - версія - переходимо в неї

```
#cd maldetect-*
```

Знаходимо та запускаємо скрипт встановлення

```
sh install.sh
```

Оновлюємо базу

```
# maldet -u
```

Можна сканувати, по замовчуванню просто створюється звіт

AI-Bolit

Find

SPAM

From:
https://wiki.djal.in/ - **IT - wiki**

Permanent link:
https://wiki.djal.in/doku.php/server/bezpeka/zlovmisni_skripti

Last update: **2020/07/09 12:25**