



Боевой OSINT

когда открытых источников не хватает

ДОКЛАДЧИК: @soxoj

v 0.0.1



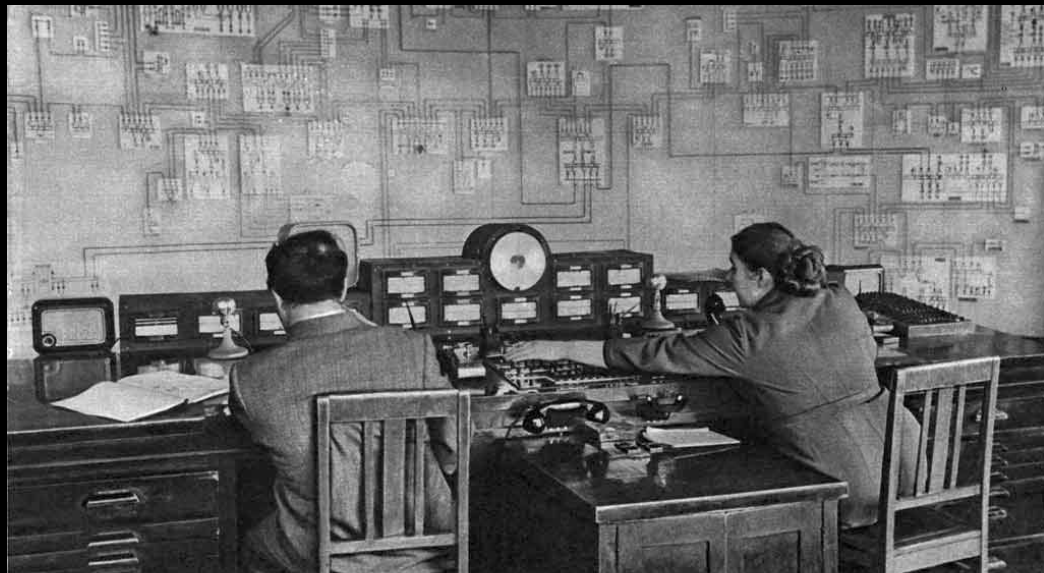
Дисклеймер

Вся информация предоставлена исключительно в ознакомительных целях. Ни организаторы, ни автор не несут ответственности за любой возможный вред, причиненный материалами данного выступления. Любые совпадения с реальными событиями и людьми случайны.



Open-source intelligence

Разведка на основе открытых источников



ЦРУ составило схему электроснабжения советской ядерной программы по фотографии из журнала “Огонёк”

Упражнение 1. Пробиваем бота Telegram

CC 2019
Боевой OSINT
c-c.ru / dc7495.org



Дано:

- исходный код с токеном бота Telegram.

Найти:

- максимум информации о владельце бота и его пользователях.



S in Telegram stands for Security

Упражнение 1. Пробиваем бота Telegram

CC 2019
Боевой OSINT
c-c.ru / dc7495.org



Дано:

- исходный код с токеном бота Telegram.

Найти:

- максимум информации о владельце бота и его пользователях.

Возможные решения:

- перебирать через API диалоги с ID, которые могут быть доступны.



S in Telegram stands for Security

Упражнение 1. Пробиваем бота Telegram

CC 2019
Боевой OSINT
c-c.ru / dc7495.org



Дано:

- исходный код с токеном бота Telegram.

Найти:

- максимум информации о владельце бота и его пользователях.

Возможные решения:

- перебирать через API диалоги с ID, которые могут быть доступны.

Дополнительная информация:

- к ботам можно подключаться напрямую через MTProto API с доступом к истории.



S in Telegram stands for Security

Упражнение 1. Пробиваем бота Telegram

CC 2019
Боевой OSINT
c-c.ru / dc7495.org



Дано:

- исходный код с токеном бота Telegram.

Найти:

- максимум информации о владельце бота и его пользователях.

Возможные решения:

- перебирать через API диалоги с ID, которые могут быть доступны.

Решение:

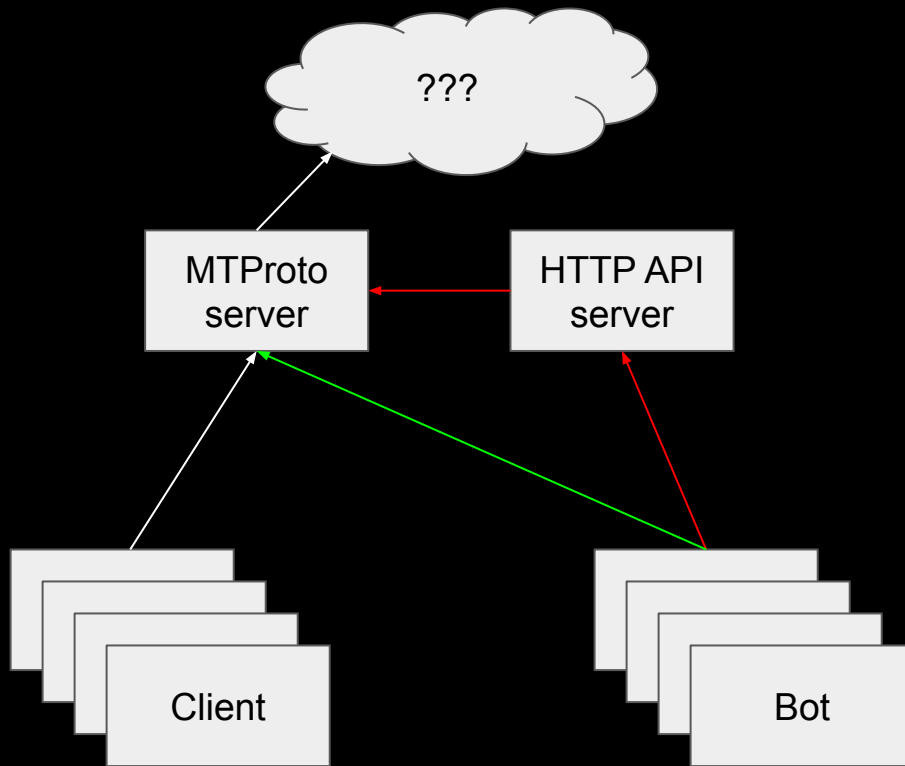
- пишем свой скрипт или используем готовый, чтобы сдампить всю историю диалогов бота;
- самый первый диалог и есть владелец, скорее всего.



S in Telegram stands for Security

<https://github.com/soxoj/telegram-bot-dumper>

Упражнение 1. Пробиваем бота Telegram



Tips & tricks:

- нельзя удалить сообщение у бота
- владелец не заметит подключения
- можно имитировать команды

Упражнение 1. Пробиваем бота Telegram

CC 2019
Боевой OSINT
c-c.ru / dc7495.org



Выводы:

- вся история ботов доступна по токену;
- не расшаривайте ботам то, что не нужно;
- делать личный таск-трекер в боте лучше не стоит;
- токены можно и нужно отзывать.



Полный доклад



S in Telegram stands for Security

Упражнение 2. Узнаем номер в ноль касаний

CC 2019
Боевой OSINT
c-c.ru / dc7495.org



Дано:

- телефон в известном радиусе рядом с вами.

Найти:

- номер телефона;
- сведения о его владельце.



Упражнение 2. Узнаем номер в ноль касаний



Дано:

- телефон в известном радиусе рядом с вами.

Найти:

- номер телефона;
- сведения о его владельце.

Возможные решения:

- СИ через подложную авторизацию в Wi-Fi;
- IMSI Catcher.



Упражнение 2. Узнаем номер в ноль касаний

CC 2019
Боевой OSINT
c-c.ru / dc7495.org



Дано:

- телефон в известном радиусе рядом с вами.

Найти:

- номер телефона;
- сведения о его владельце.

Возможные решения:

- СИ через подложную авторизацию в Wi-Fi;
- IMSI Catcher.

Дополнительная информация:

- iPhone.



Apple bleee

Упражнение 2. Узнаем номер в ноль касаний



Дано:

- телефон в известном радиусе рядом с вами.

Найти:

- номер телефона;
- сведения о его владельце.

Возможные решения:

- СИ через подложную авторизацию в Wi-Fi;
- IMSI Catcher.

Дополнительная информация:

- iPhone.

Найти:

- используем Apple blee для перехвата начала хэшей телефона, почты, Apple ID;
- по хэшу определяем десяток возможных номеров, пробиваем через HLR, мессенджеры;
- используем хэши для верификации остальных данных.



Apple blee

Упражнение 2. Узнаем номер в ноль касаний

CC 2019
Боевой OSINT
c-c.ru / dc7495.org



Apple devices scanner

Mac	State	Device	WI-FI	OS	Phone	Time
66:F5:D5:6B:29:	Off	iPhone	Off	iOS12		1566074720
3C:CD:5D:C4:06:	Home screen	iPhone	Off	iOS12		1566074667
76:20:C5:6D:DB:	Home screen	iPhone	On	iOS12		1566074714
49:0D:3D:2C:2F:	Off	iPhone	On	iOS12		1566074724
48:11:D1:2D:6B:	Home screen	iPhone	On	iOS12		1566074723
4A:54:4F:AC:24:	Off	iPhone	On	iOS12		1566074724
63:F6:6D:BA:43:	Off	iPhone	Off	iOS12		1566074724
6A:0F:EE:D2:B2:	Off	iPhone	Off	iOS12		1566074723
6B:C1:9E:03:90:	Off	iPhone	On	iOS12		1566074723
49:F2:B5:10:38:	LR:in	AirPods	<none>	<none>	<none>	1566074723
7A:49:EF:E3:80:	Lock screen	iPhone	On	iOS12		1566074725
0E:71:83:4B:68:	Off	iPhone	On	iOS12		1566074720
71:CF:87:E7:02:	Home screen	iPhone	<unknown>	iOS10		1566074723
76:70:AC:1D:BB:	LR:in	AirPods	<none>	<none>	<none>	1566074720
5D:98:EF:07:9A:	LR:in	AirPods	<none>	<none>	<none>	1566074726
55:51:3D:F5:95:	Home screen	iPhone	Off	iOS12		1566074725
42:CA:2A:4F:53:	Home screen	iPhone	Off	iOS12		1566074721
7D:E8:8A:30:3E:	Off	iPhone	On	iOS12		1566074716
4C:23:1A:97:53:	LR:in	AirPods	<none>	<none>	<none>	1566074724

Упражнение 2. Узнаем номер в ноль касаний

CC 2019
Боевой OSINT
c-c.ru / dc7495.org



Выводы:

- удобство достигается потерей полной приватности;
- вы можете слышать и спуфать общение между любыми устройствами Apple рядом.



Apple bleee

<https://habr.com/ru/post/351114/>

Упражнение 3. Поиск аккаунта через коннект к SSH

CC 2019
Боевой OSINT
c-c.ru / dc7495.org

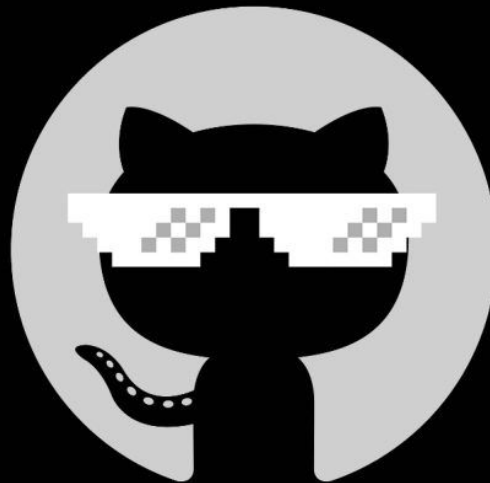


Дано:

- человек с претензией на умение кодить.

Найти:

- профили на GitHub/Gitlab;
- email-адреса.



Упражнение 3. Поиск аккаунта через коннект к SSH

CC 2019
Боевой OSINT
c-c.ru / dc7495.org



Дано:

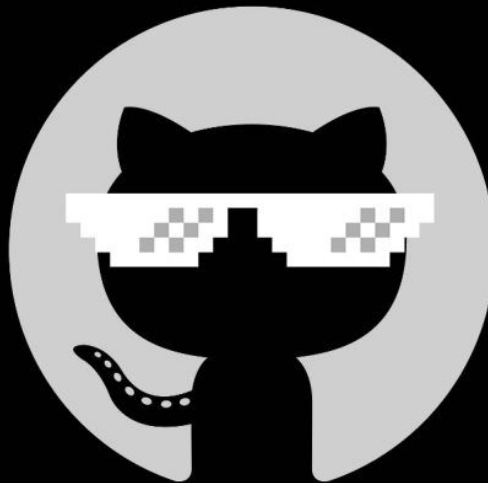
- человек с претензией на умение кодить.

Найти:

- профили на GitHub/Gitlab;
- email-адреса.

Возможные решения:

- поиск по никнейму;
- поиск по коду.



Упражнение 3. Поиск аккаунта через коннект к SSH

CC 2019
Боевой OSINT
c-c.ru / dc7495.org



Дано:

- человек с претензией на умение кодить.

Найти:

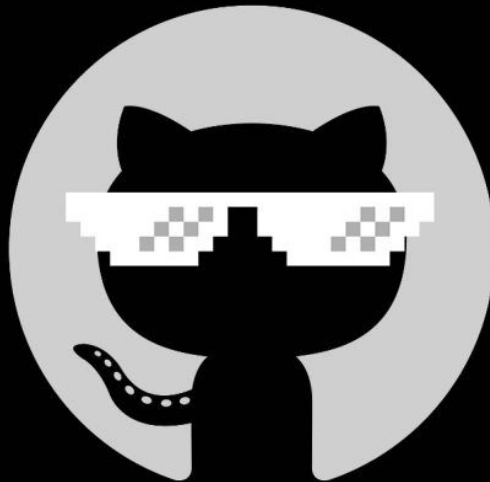
- профили на GitHub/Gitlab;
- email-адреса.

Возможные решения:

- поиск по никнейму;
- поиск по коду.

Дополнительная информация:

- человек интересуется серверами с паролями по умолчанию;
- публичные ключи SSH профилей в GitHub и Gitlab общедоступны и легко парсятся.



Упражнение 3. Поиск аккаунта через коннект к SSH

CC 2019
Боевой OSINT
c-c.ru / dc7495.org



Дано:

- человек с претензией на умение кодить.

Найти:

- профили на GitHub/Gitlab;
- email-адреса.

Возможные решения:

- поиск по никнейму;
- поиск по коду.

Решение:

- собираем базы SSH-ключей / ссылок на профили;
- подкидываем адрес нашего сервера с SSH;
- логируем все публичные ключи, которые перебираются для подключения;
- ищем по ключам профили;
- вытаскиваем почтовые адреса из кода.



Упражнение 3. Поиск аккаунта через коннект к SSH

CC 2019
Боевой OSINT
c-c.ru / dc7495.org



```
$ ssh whoami.filippo.io
```

<https://gitlab.com/USERNAME.keys>

<https://github.com/USERNAME.keys>



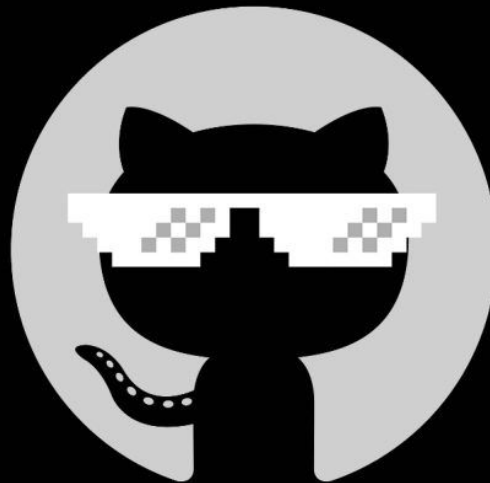
Упражнение 3. Поиск аккаунта через коннект к SSH

CC 2019
Боевой OSINT
c-c.ru / dc7495.org



Выводы:

- нужно бережнее относиться к SSH и настраивать пары ключ / сервер отдельно;
- не стоит коммитить рабочий код с домашней машины и наоборот.



Упражнение 4. Скелеты в Telegram-шкафу

CC 2019
Боевой OSINT
c-c.ru / dc7495.org

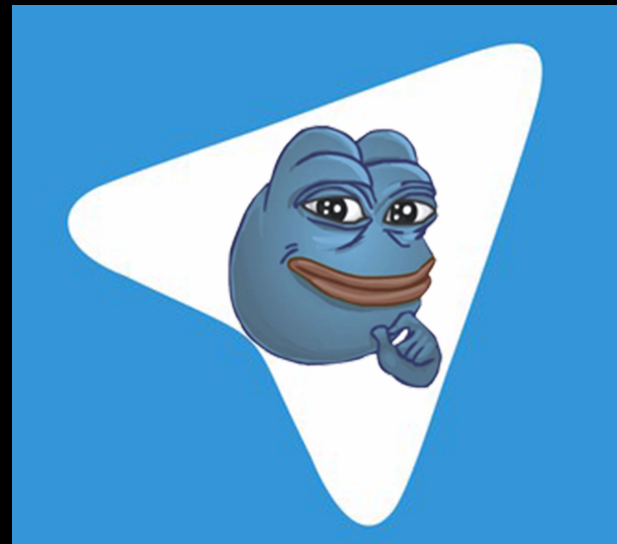


Дано:

- аккаунт, недавно сменивший имя и юзернейм.

Найти:

- максимум информации о пользователе, желательно полный профиль.



Упражнение 4. Скелеты в Telegram-шкафу



Дано:

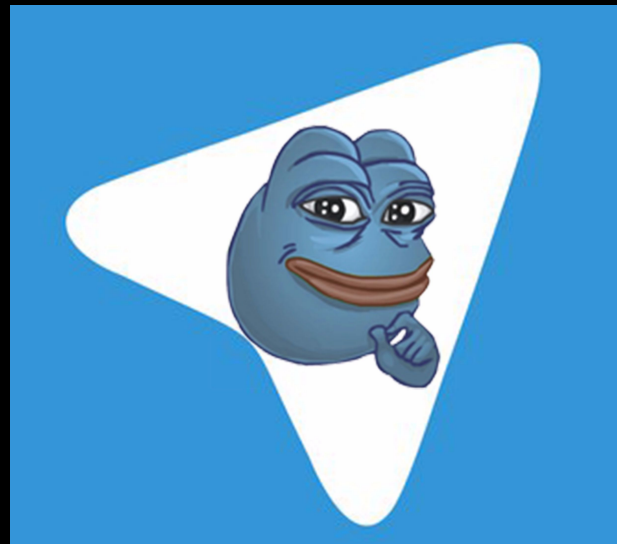
- аккаунт, недавно сменивший имя и юзернейм.

Найти:

- максимум информации о пользователе, желательно полный профиль.

Возможные решения:

- поиск по имени в search.buzz.im;
- поиск по ID (@userinfobot);
- использование групповых ботов.



Упражнение 4. Скелеты в Telegram-шкафу



Дано:

- аккаунт, недавно сменивший имя и юзернейм.

Найти:

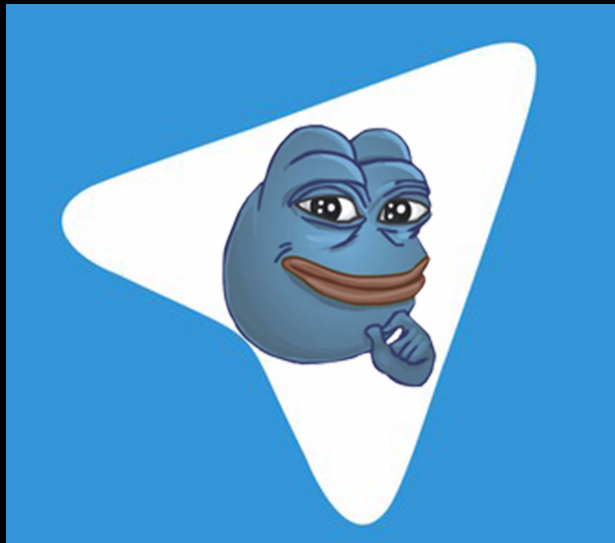
- максимум информации о пользователе, желательно полный профиль.

Возможные решения:

- поиск по имени в search.buzz.im;
- поиск по ID (@userinfobot);
- использование групповых ботов.

Дополнительная информация:

- **SQLi в саджете поиска пользователя на сайте бота для проверки кармы.**



Упражнение 4. Скелеты в Telegram-шкафу



Дано:

- аккаунт, недавно сменивший имя и юзернейм.

Найти:

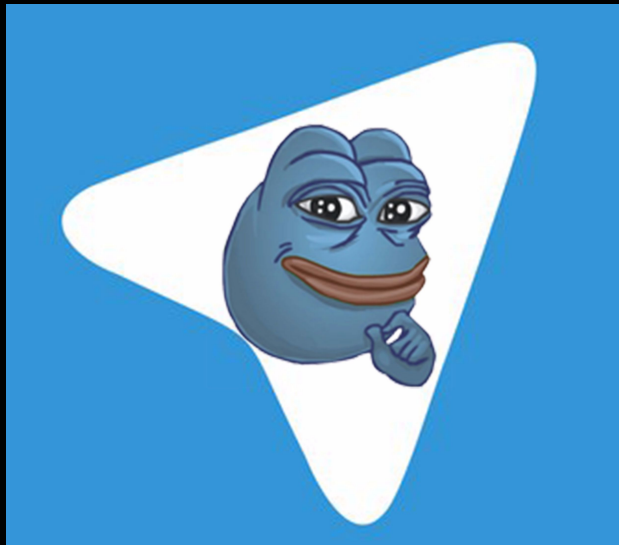
- максимум информации о пользователе, желательно полный профиль.

Возможные решения:

- поиск по имени в search.buzz.im;
- поиск по ID (@userinfobot);
- использование групповых ботов.

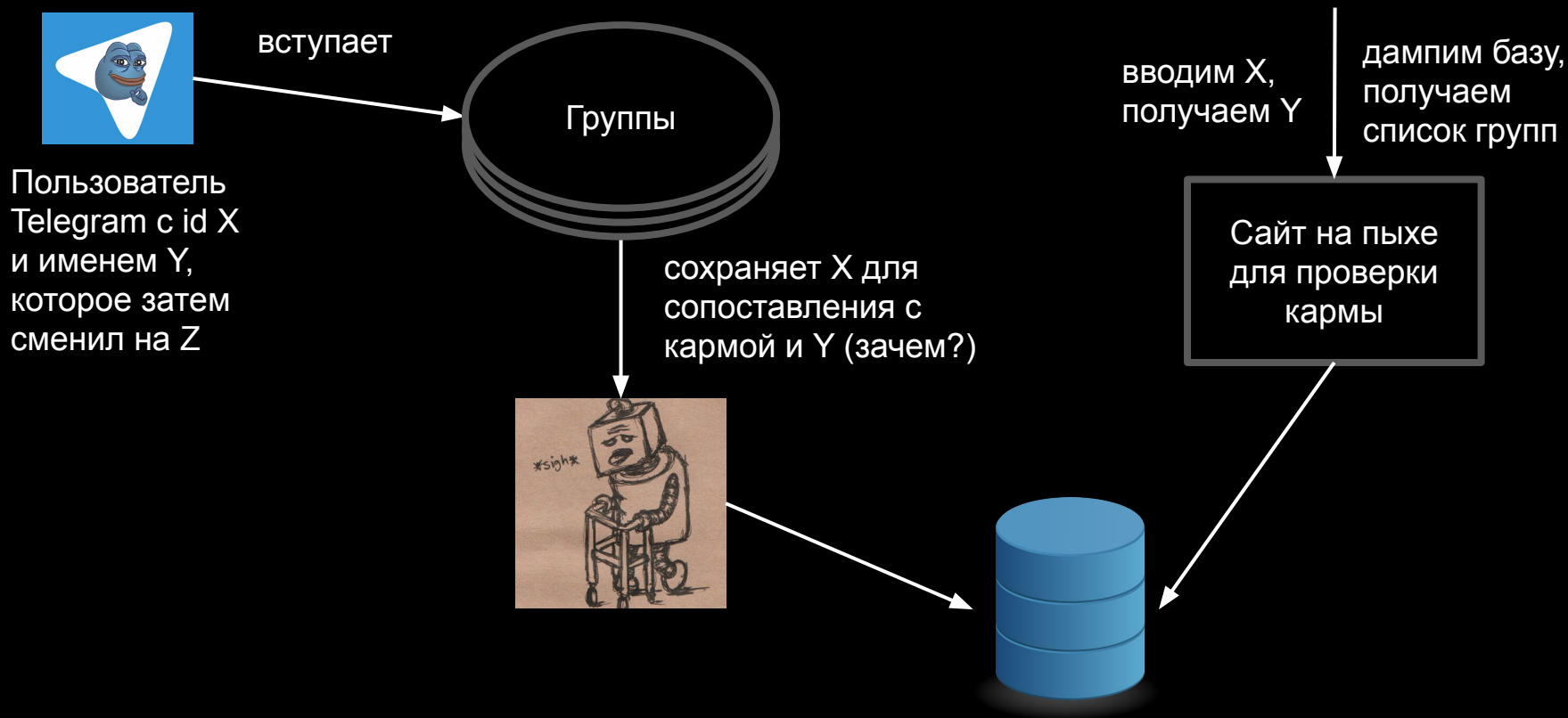
Решение:

- вытаскиваем всю возможную информацию из автодополнения строки поиска;
- вытаскиваем всю невозможную информацию напрямую из базы.



Упражнение 4. Скелеты в Telegram-шкафу

CC 2019
Боевой OSINT
c-c.ru / dc7495.org



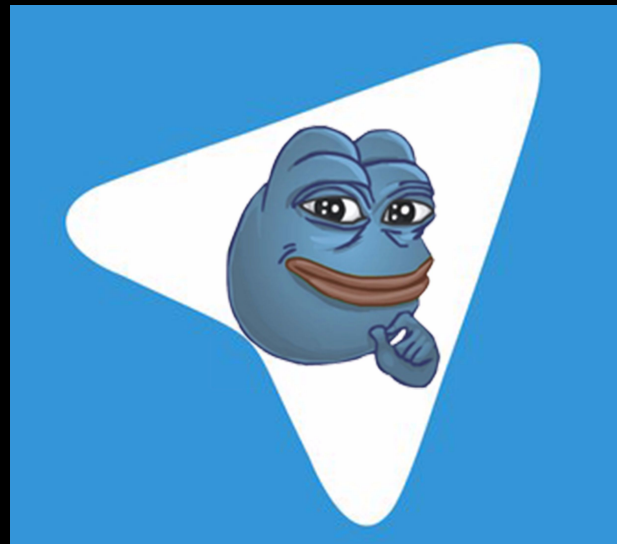
Упражнение 4. Скелеты в Telegram-шкафу

CC 2019
Боевой OSINT
c-c.ru / dc7495.org



Выводы:

- от треканья не скраться нигде, даже в мессенджерах;
- все любят собирать себе лишние данные - пригодятся;
- побочная функциональность чаще всего заботована.



Упражнение 5. Скрытые данные профиля



Дано:

- минимум информации по человеку;
- аккаунт на форуме;
- данные аккаунта скрыты от остальных.

Найти:

- email аккаунта;
- все остальные данные аккаунта.



Упражнение 5. Скрытые данные профиля



Дано:

- минимум информации по человеку;
- аккаунт на форуме;
- данные аккаунта скрыты от остальных.

Найти:

- email аккаунта;
- все остальные данные аккаунта.

Возможные решения:

- утечки базы форума;
- поиск аккаунтов на других сайтах.



Вы еще не открыли
этого персонажа!

Упражнение 5. Скрытые данные профиля



Дано:

- минимум информации по человеку;
- аккаунт на форуме;
- данные аккаунта скрыты от остальных.

Найти:

- email аккаунта;
- все остальные данные аккаунта.

Дополнительная информация:

- XSS в поле "Телефон".



Упражнение 5. Скрытые данные профиля



Дано:

- минимум информации по человеку;
- аккаунт на форуме;
- данные аккаунта скрыты от остальных.

Найти:

- email аккаунта;
- все остальные данные аккаунта.

Дополнительная информация:

- XSS в поле "Телефон".

Решение:

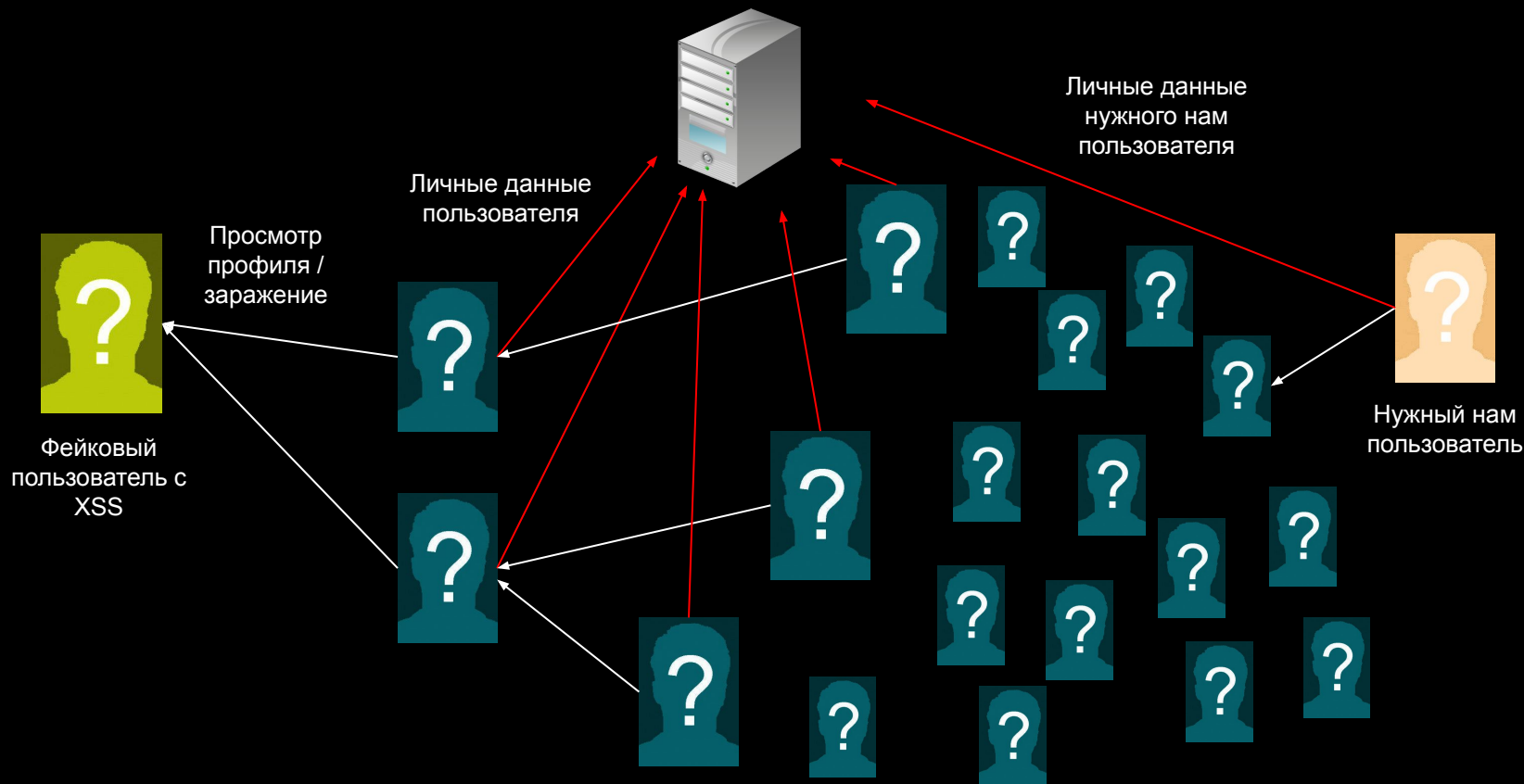
- пишем скрипт и внедряем к себе на страницу;
 - отправляет данные пользователя нам на сервер;
 - дописывает себя в поле пользователю;
- пишем максимально привлекающее внимание сообщение;
- ...
- PROFIT



Вы еще не открыли
этого персонажа!

Упражнение 5. Скрытые данные профиля

CC 2019
Боевой OSINT
c-c.ru / dc7495.org



Упражнение 5. Скрытые данные профиля

CC 2019
Боевой OSINT
c-c.ru / dc7495.org



Выводы:

- вирусное распространение ускоряет СИ;
- иногда нужно везение, много везения.



Вы еще не открыли
этого персонажа!



The End

СПАСИБО. ВОПРОСЫ?