15x4

Атака на браузеры

Александр

О чем поговорим?

HTTP(S), MiTM, XSS, WiFi

A

B

E

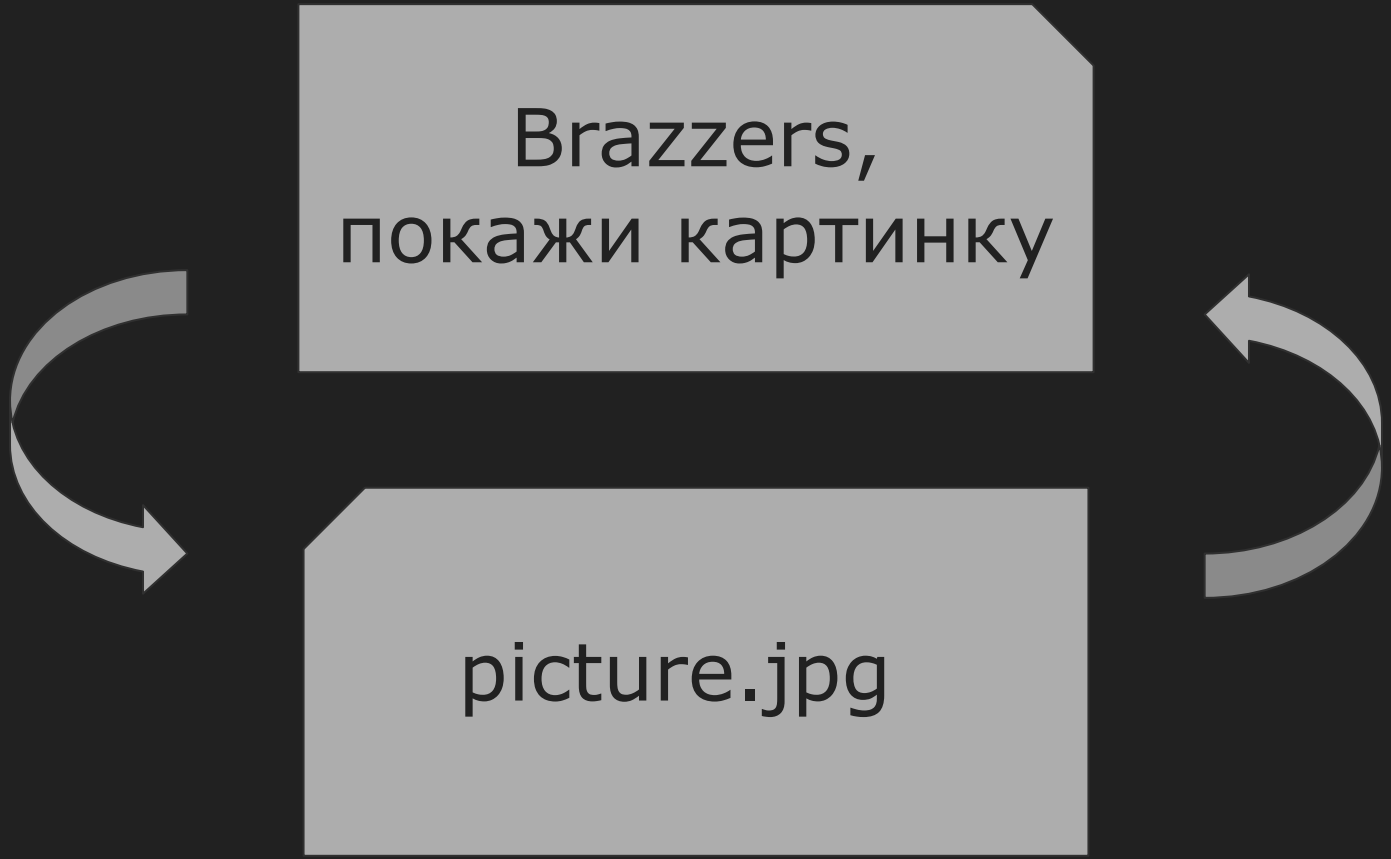
Антон

BRAZZERS

Евгений

HTTP

Hyper Text Transport Protocol


Brazzers,
покажи картинку
picture.jpg

HTTP-Пакет (запрос)

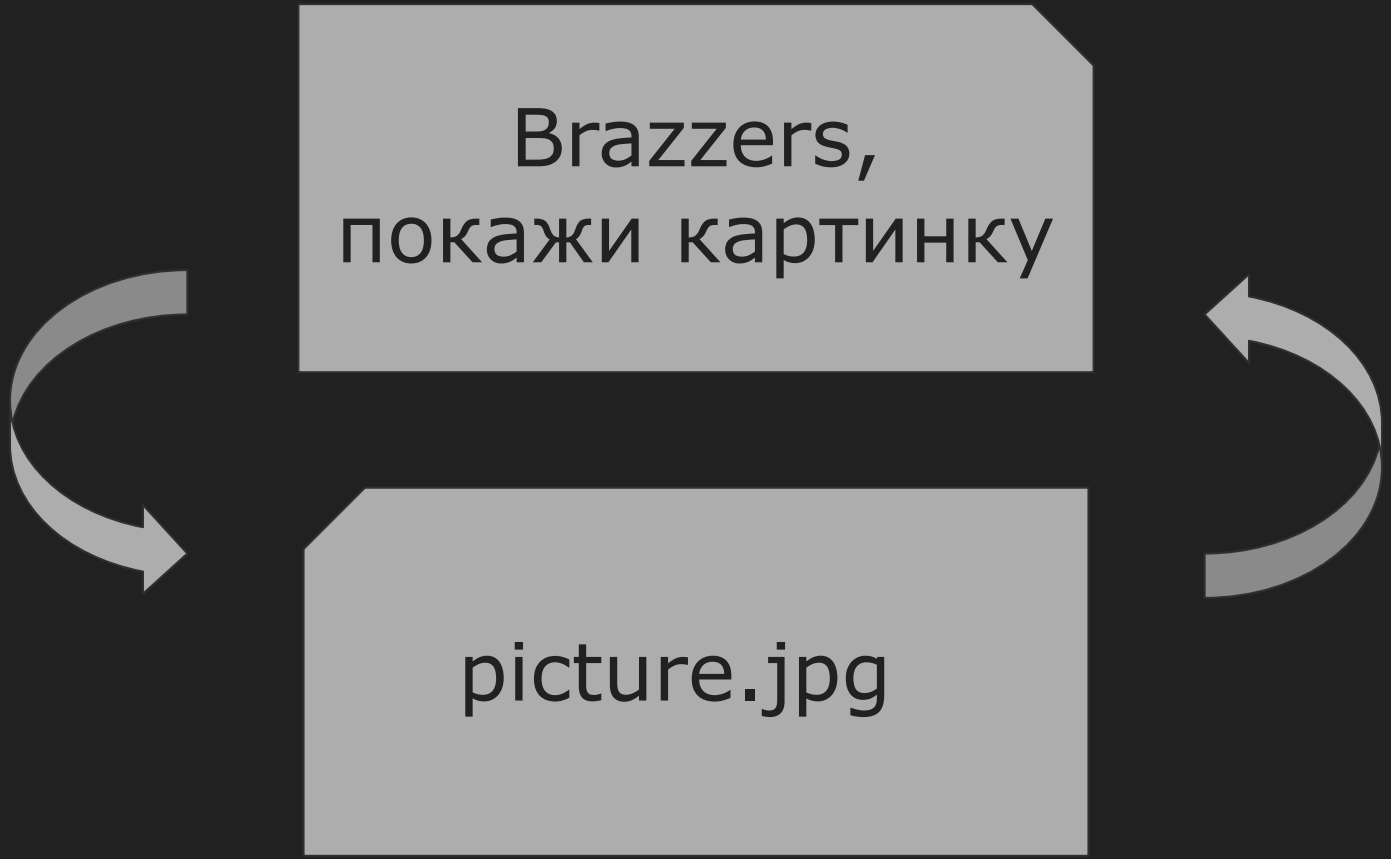
Привет, Brazzers. Есть главная страница?

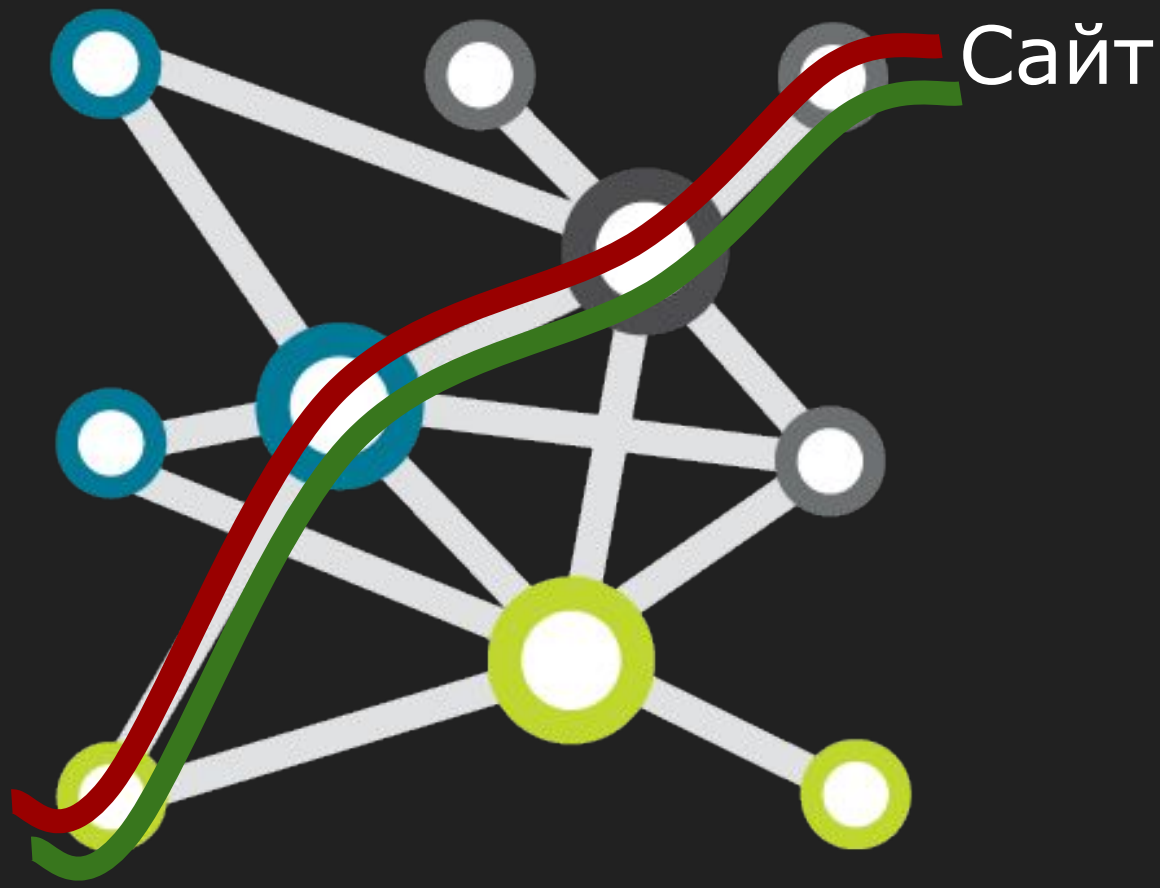
HTTP-Пакет (ответ)

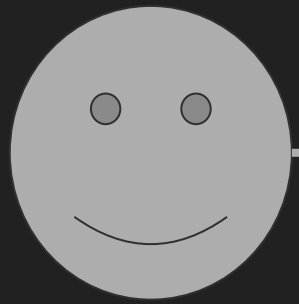
```
<html>
   Welcome!
   ...
</html>
```

Это был HTTP в двух слайдах

Да, все так просто


Brazzers,
покажи картинку
picture.jpg

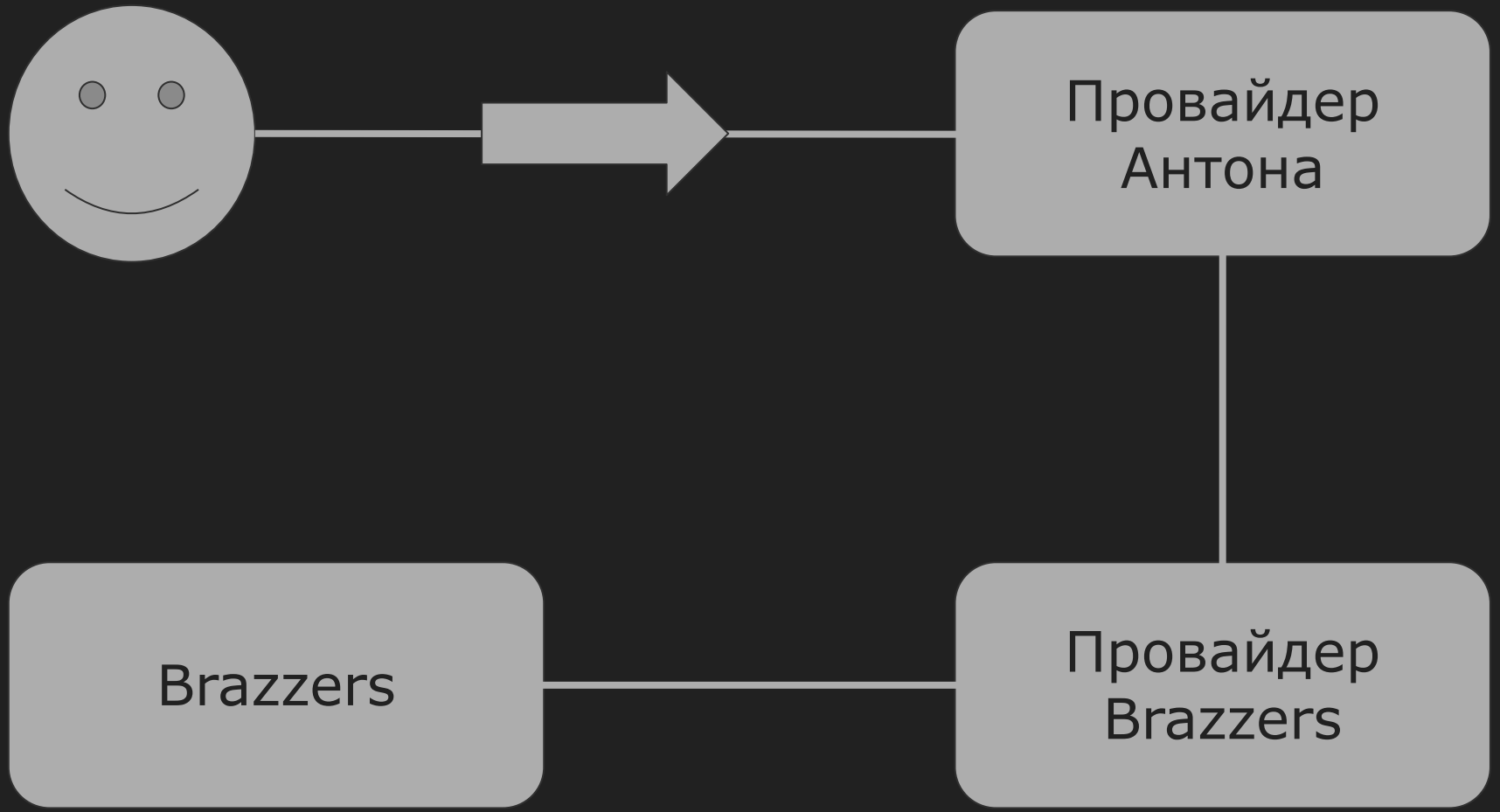

Сайт
Браузер

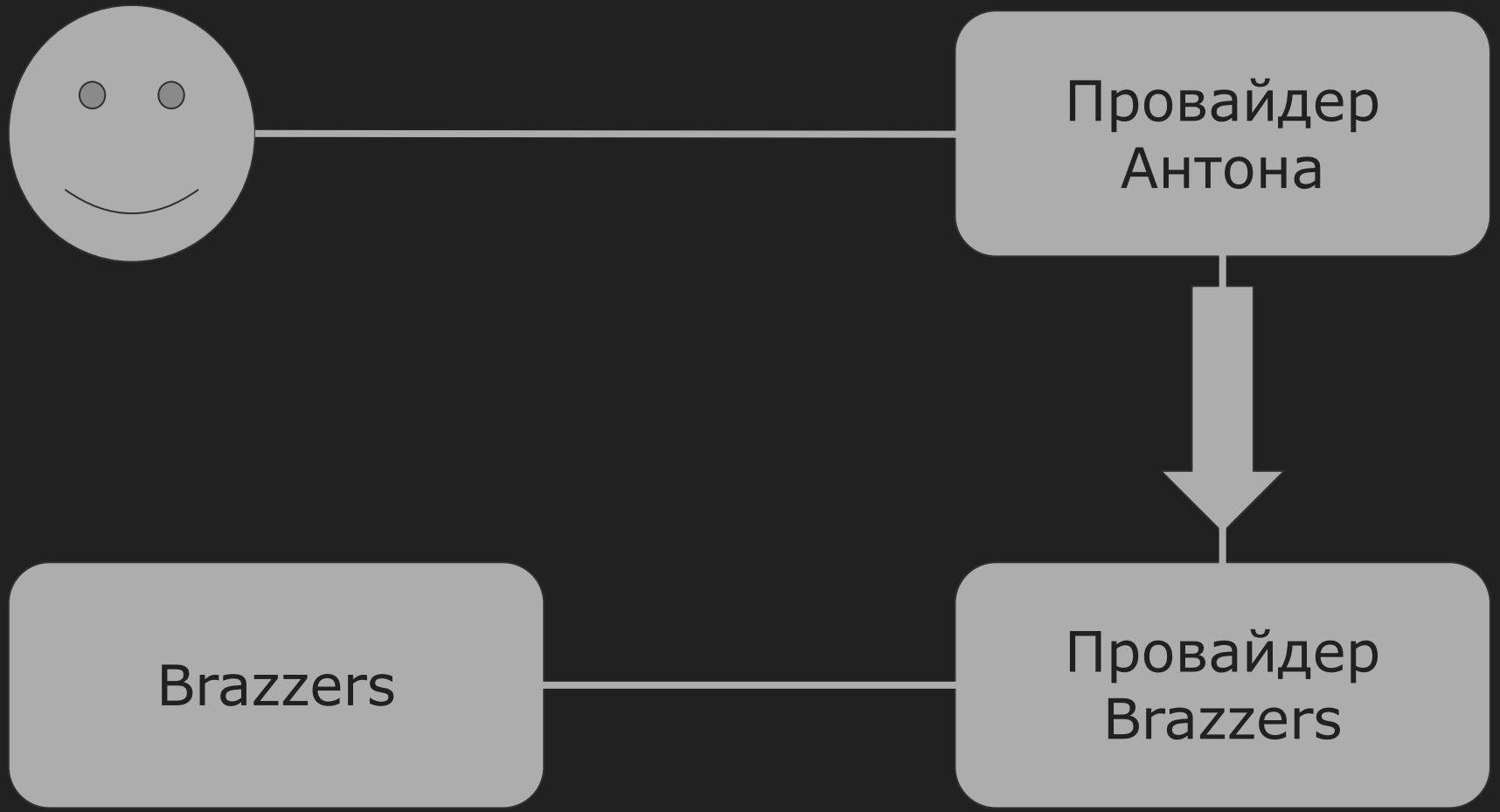


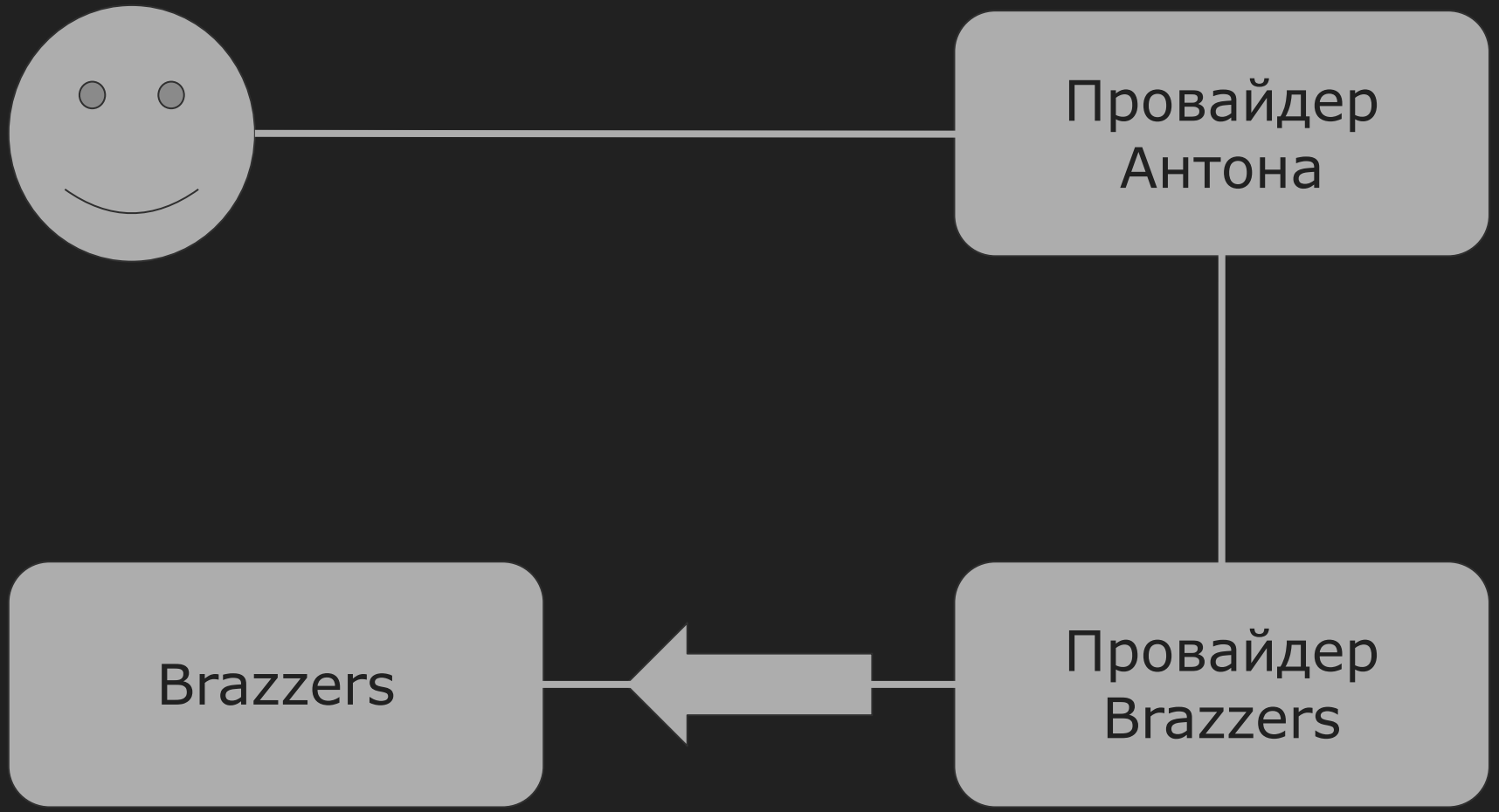
Провайдер Антона

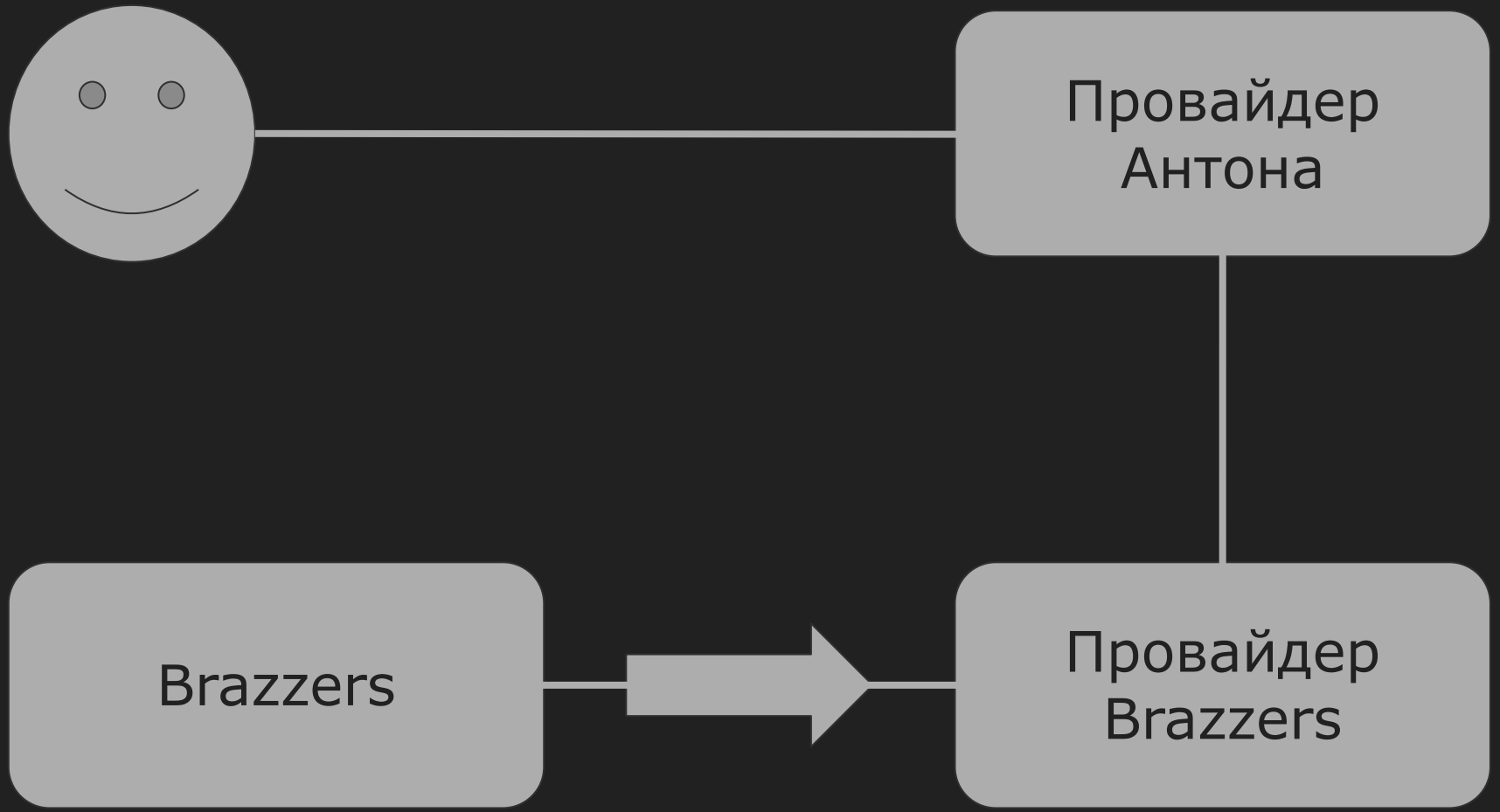
Brazzers

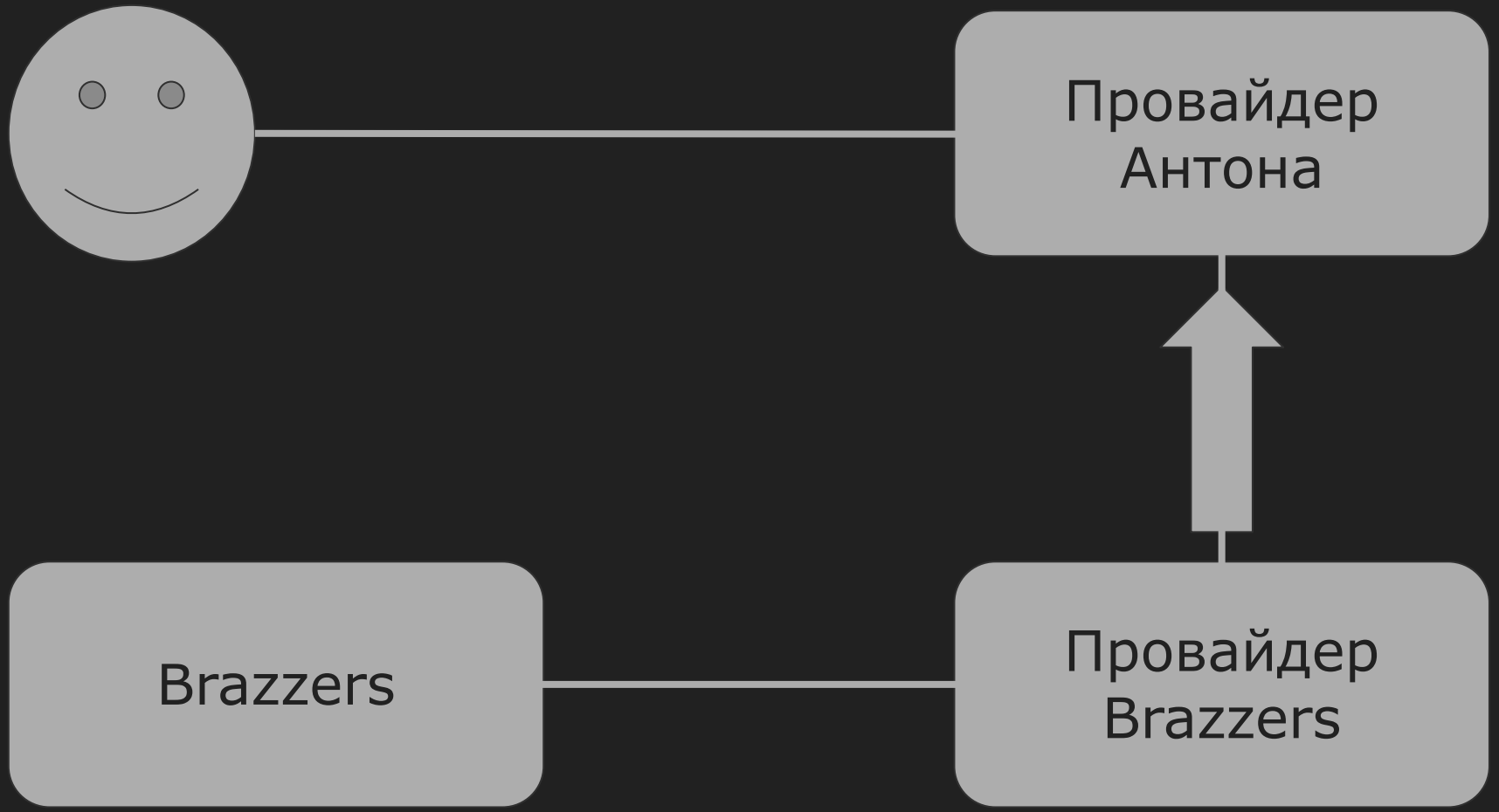
Провайдер Brazzers

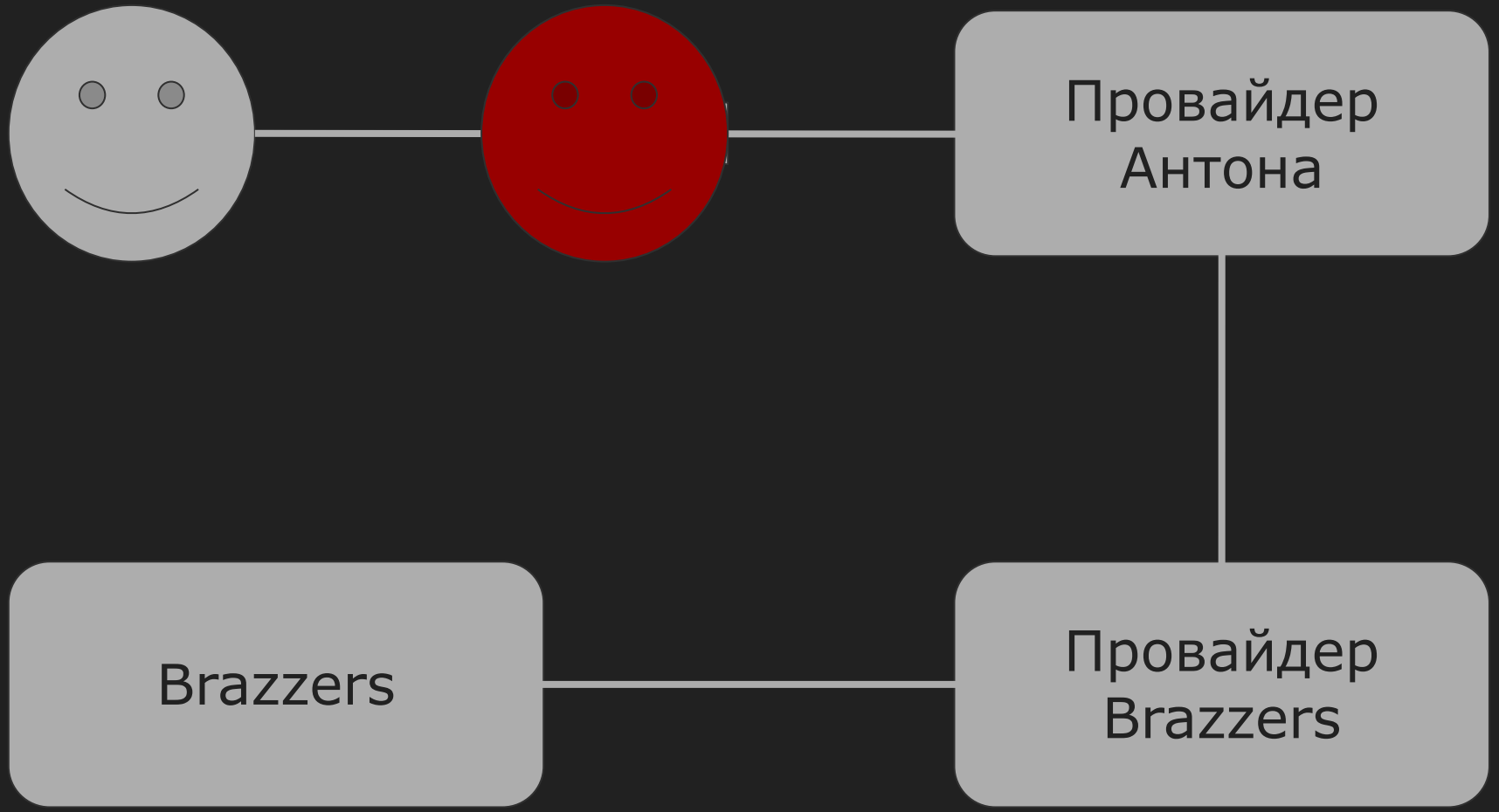

Провайдер
Антона
Brazzers
Провайдер
Brazzers


Провайдер
Антона
Brazzers
Провайдер
Brazzers


Провайдер
Антона
Brazzers
Провайдер
Brazzers


Провайдер
Антона
Brazzers
Провайдер
Brazzers


Провайдер
Антона
Brazzers
Провайдер
Brazzers

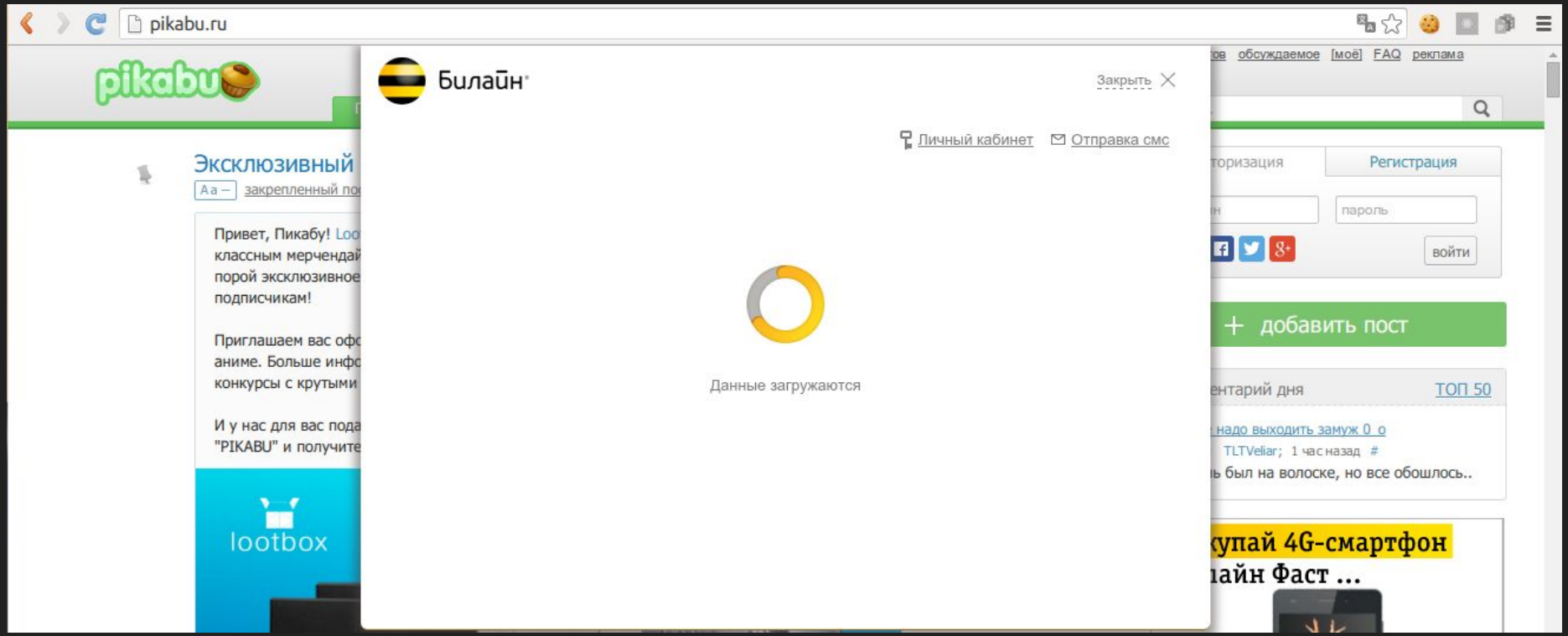

Провайдер
Антона
Brazzers
Провайдер
Brazzers

Это был MiTM* HTTP

*MiTM — Man in The Middle**

Man in The Middle — Человек в середине*

***Или Monkey in The Middle — Что говорит о популярности атаки


pikabu.ru
pikabu
обсуждаемое
[моё]
FAQ
реклама
Эксклюзивный
Привет, Пикабу!
подписчикам!
Приглашаем вас
аниме. Больше
конкурсы с крутыми
И у нас для вас
"PIKABU" и получите
lootbox
Билайн
Закрыть
Личный кабинет
Отправка смс
Данные загружаются
Регистрация
пароль
войти
добавить пост
ТОП 50
надо выходить замуж 0_о
TLTVeliar; 1 час назад #
был на волоске, но все обошлось..
купай 4G-смартфон
айн Фаст ...

HTTPS

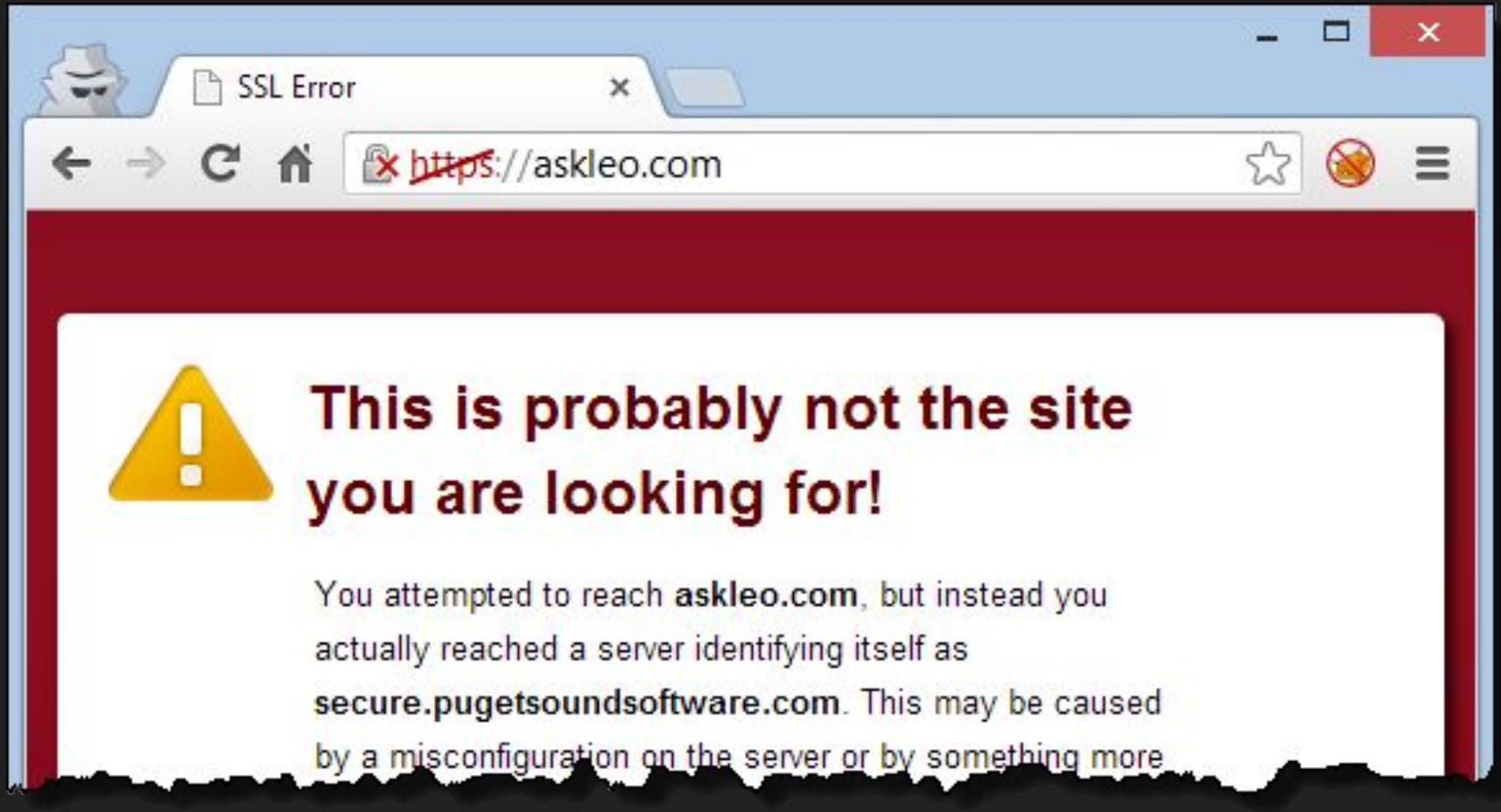
HTTPSecure

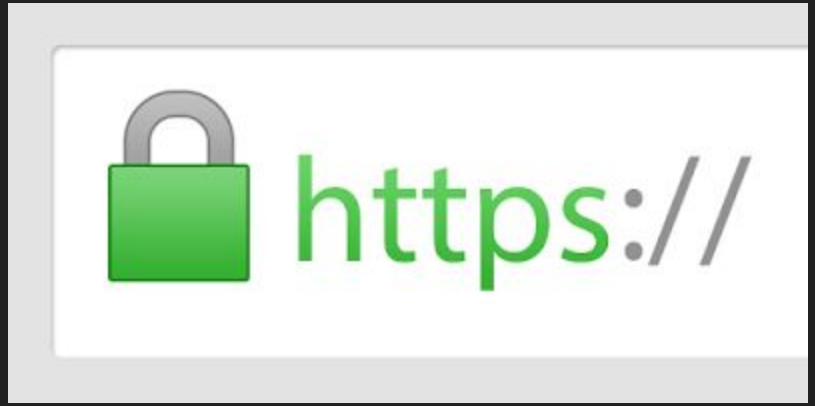
HTTP-Пакет (запрос)

Привет, Brazzers. Есть главная страница?

HTTPS-Пакет (запрос)

`B 7E`V `×`N`M À t% z7E`N
r#`N zj¸# `×`N`M


SSL Error
https://askleo.com
This is probably not the site you are looking for!
You attempted to reach askleo.com, but instead you actually reached a server identifying itself as secure.pugetsoundsoftware.com. This may be caused by a misconfiguration on the server or by something more


https://

HTTPS

HTTP

HTTP

HTTPS — твой бро*

*Но это не точно

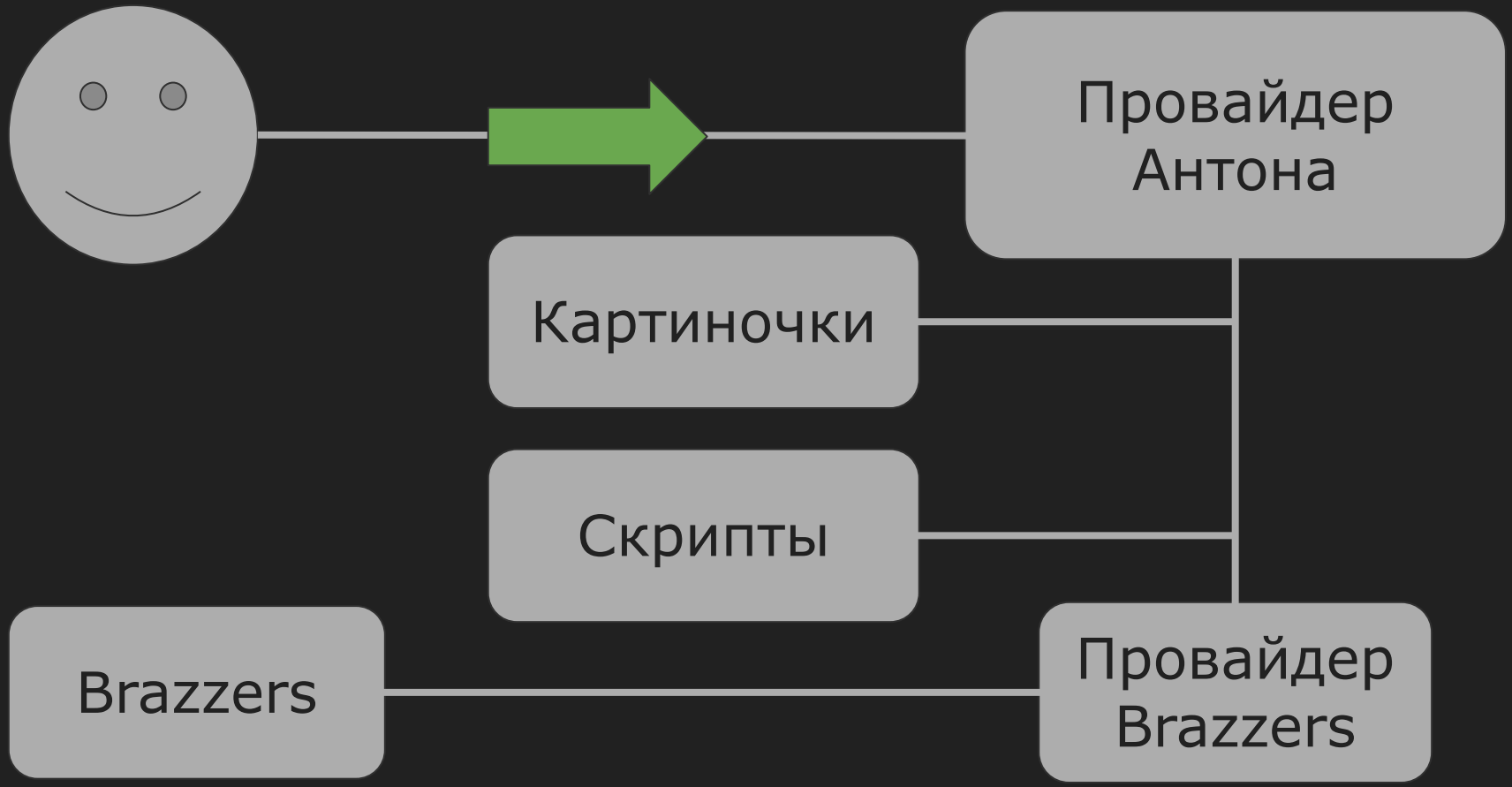
Казахстан-Style

Уважаемый Абонент!

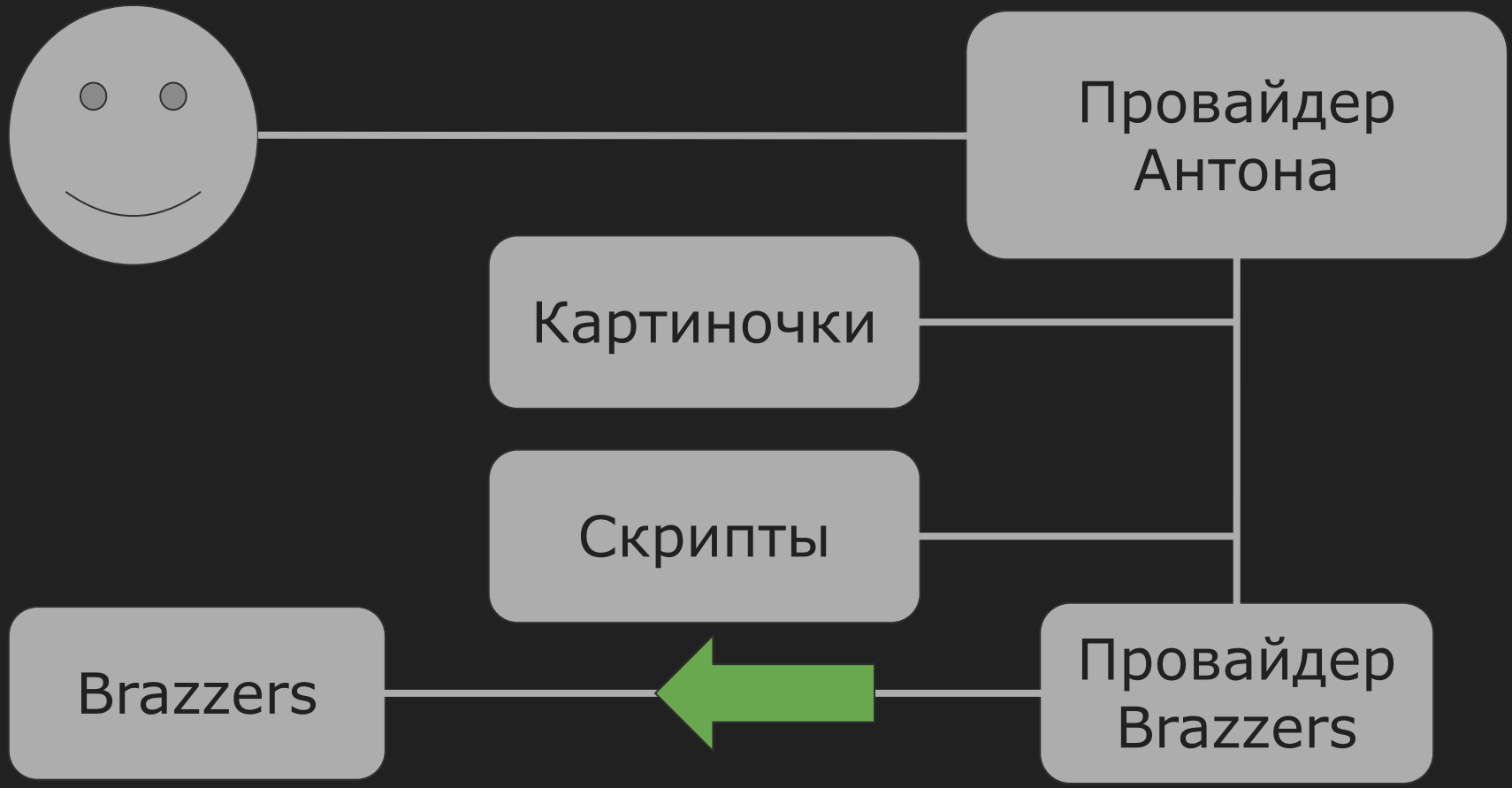
С 1 января 2016 года в соответствии с Законом Республики Казахстан «О внесении изменений и дополнений в некоторые законодательные акты Республики Казахстан по вопросам информатизации» от 24 ноября 2015 года № 419-V ЗРК Комитет связи, информатизации и информации Министерства по инвестициям и развитию Республики Казахстан внедряет национальный сертификат безопасности для пользователей сети Интернет.

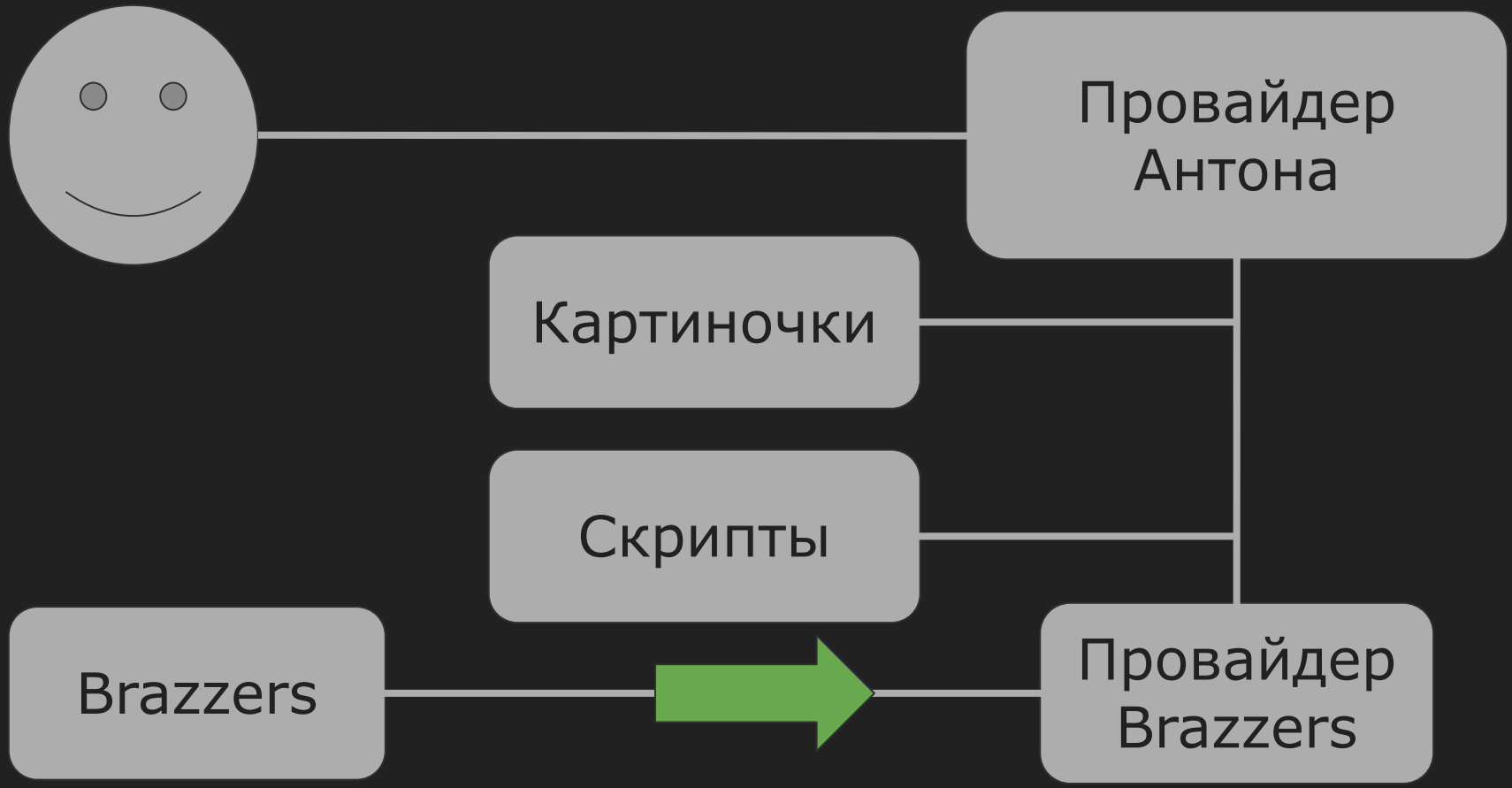
Сертификат безопасности

Пару минут спустя

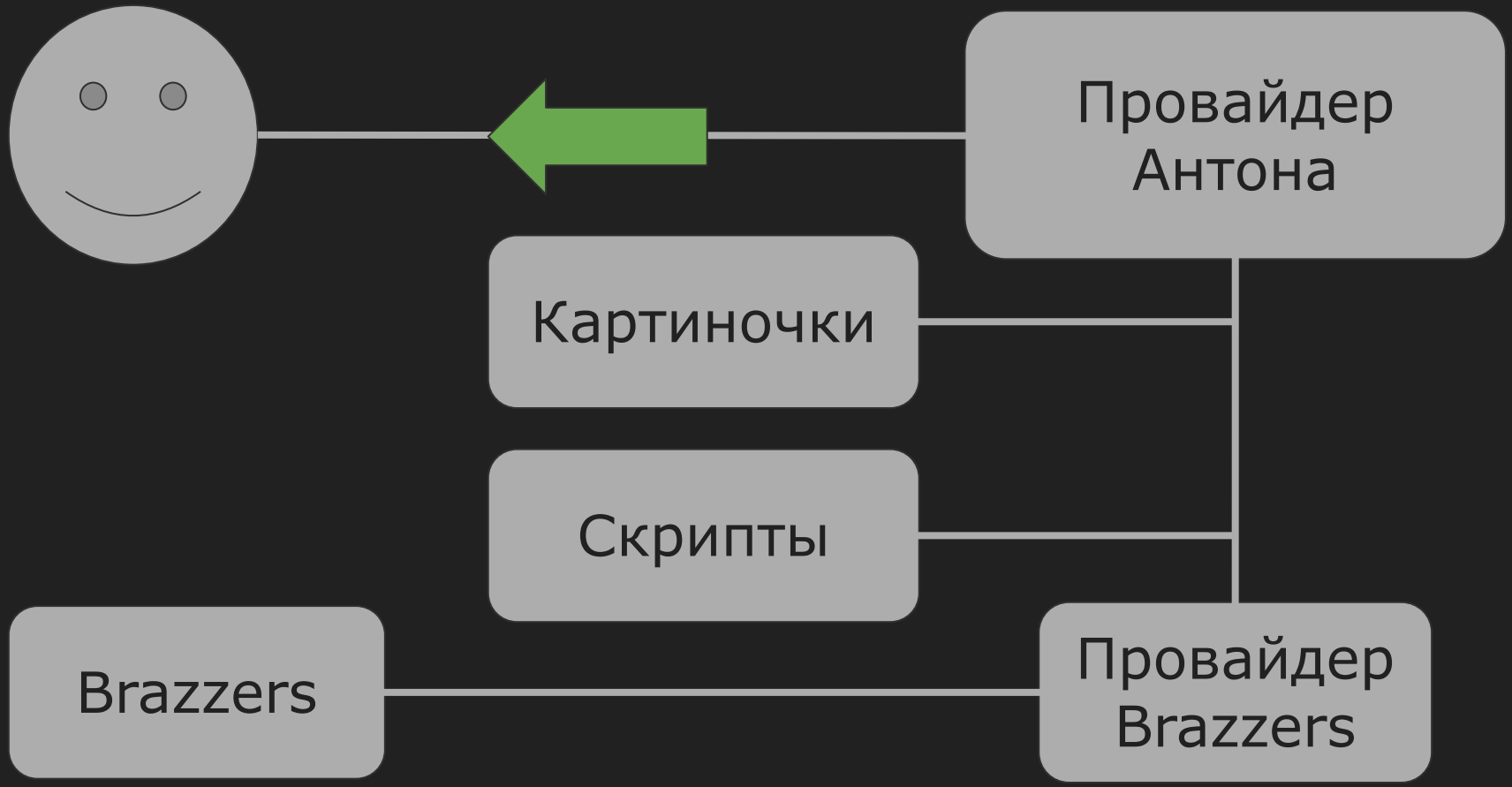

Провайдер
Антона
Картиночки
Скрипты
Brazzers
Провайдер
Brazzers


Провайдер Антона
Картиночки
Скрипты
Brazzers
Провайдер Brazzers

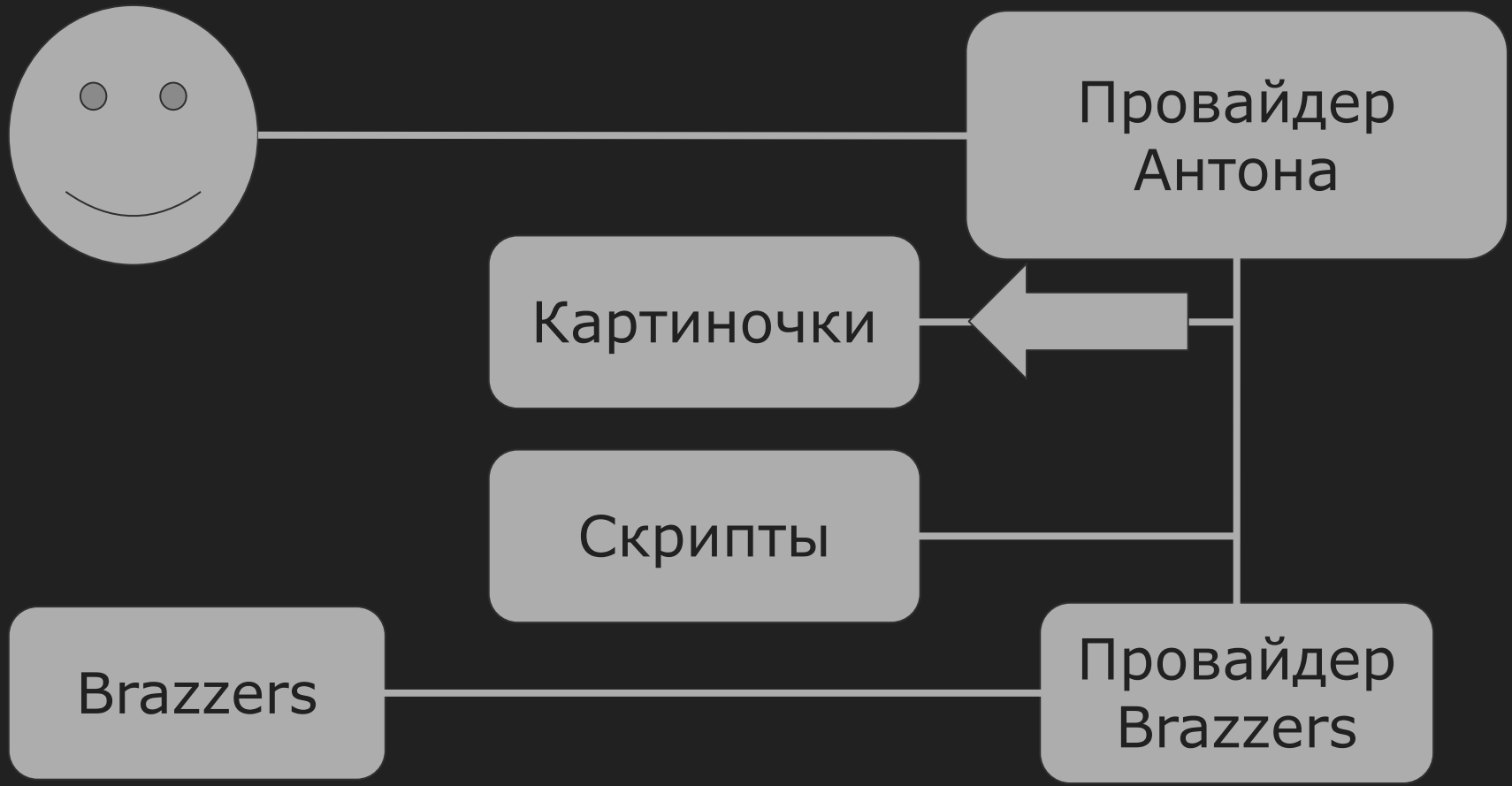

Провайдер
Антона
Картиночки
Скрипты
Brazzers
Провайдер
Brazzers

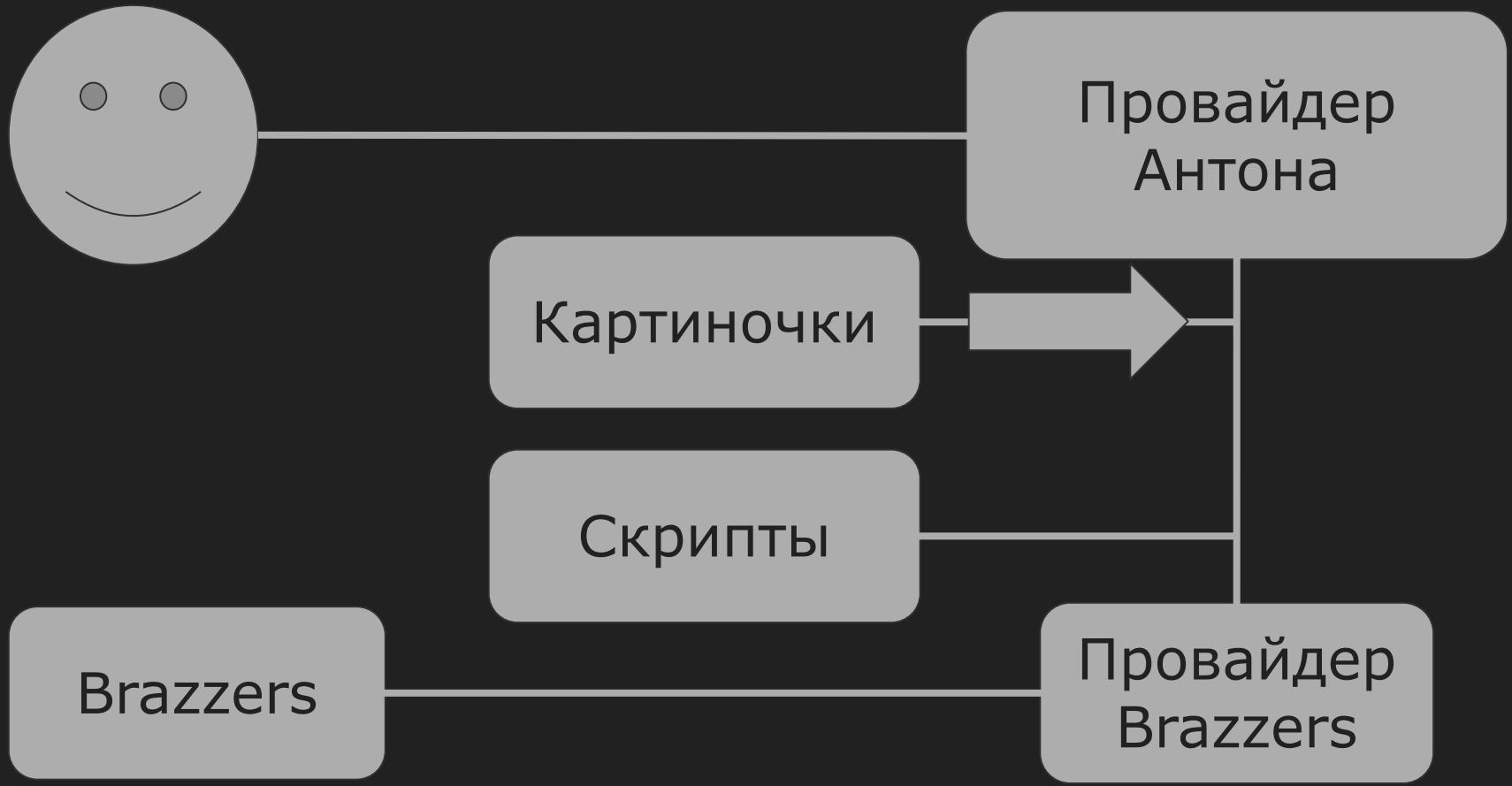

Провайдер
Антона
Картиночки
Скрипты
Brazzers
Провайдер
Brazzers


Провайдер
Антона
Картиночки
Скрипты
Brazzers
Провайдер
Brazzers


Провайдер
Антона
Картиночки
Скрипты
Brazzers
Провайдер
Brazzers


Провайдер
Антона
Картиночки
Скрипты
Brazzers
Провайдер
Brazzers

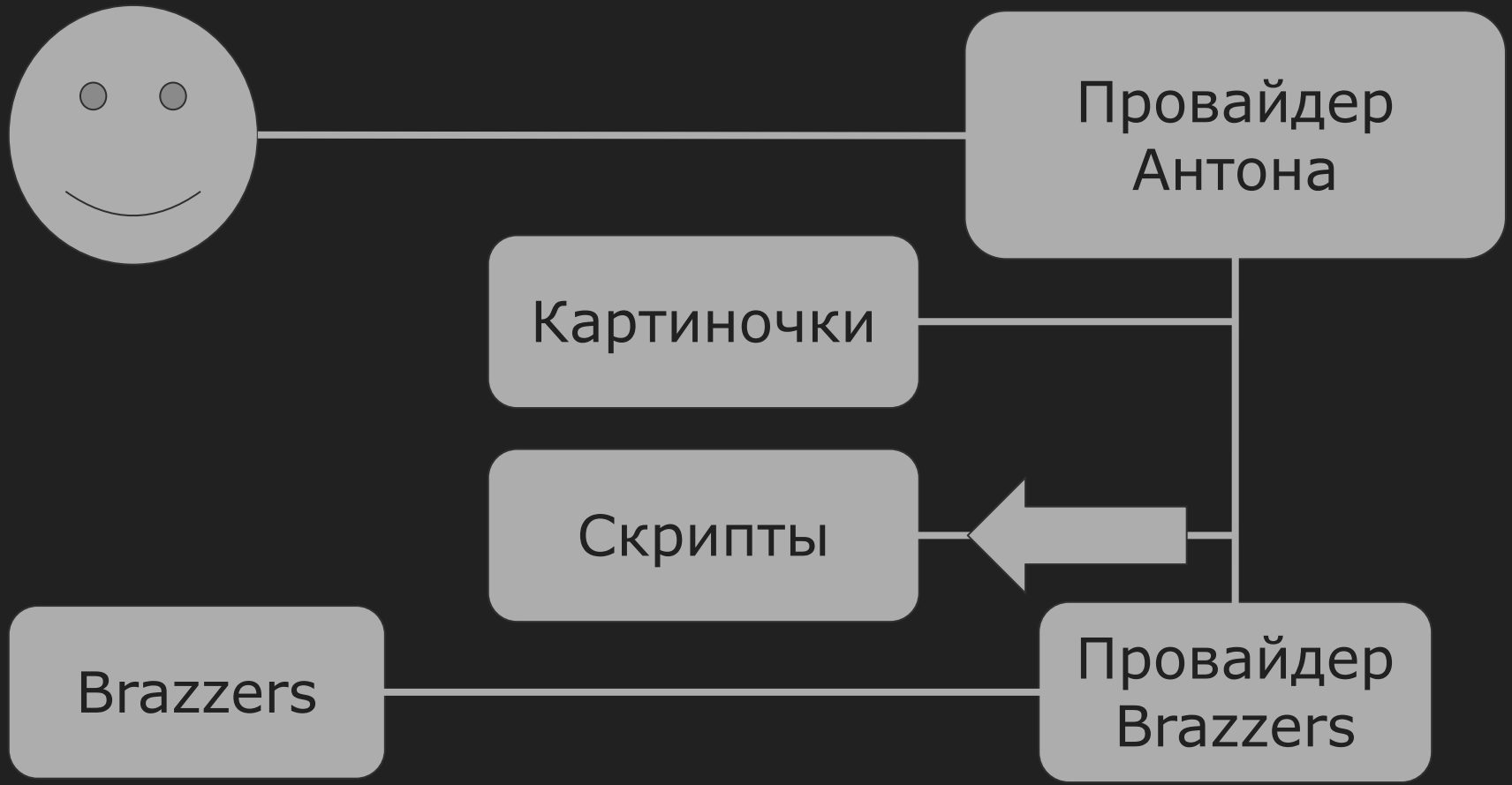

Провайдер
Антона
Картиночки
Скрипты
Brazzers
Провайдер
Brazzers

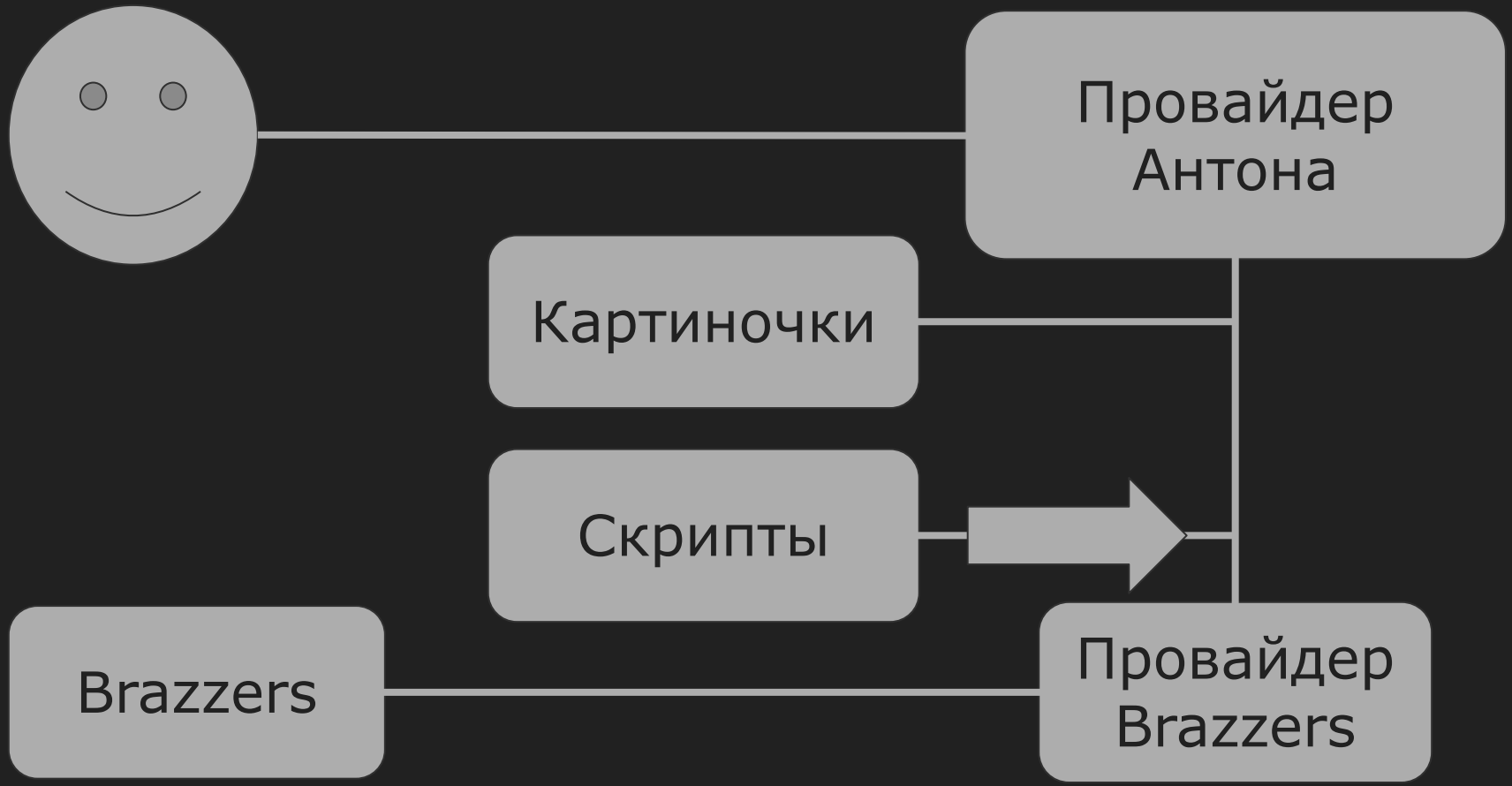

Провайдер
Антона
Картиночки
Скрипты
Brazzers
Провайдер
Brazzers

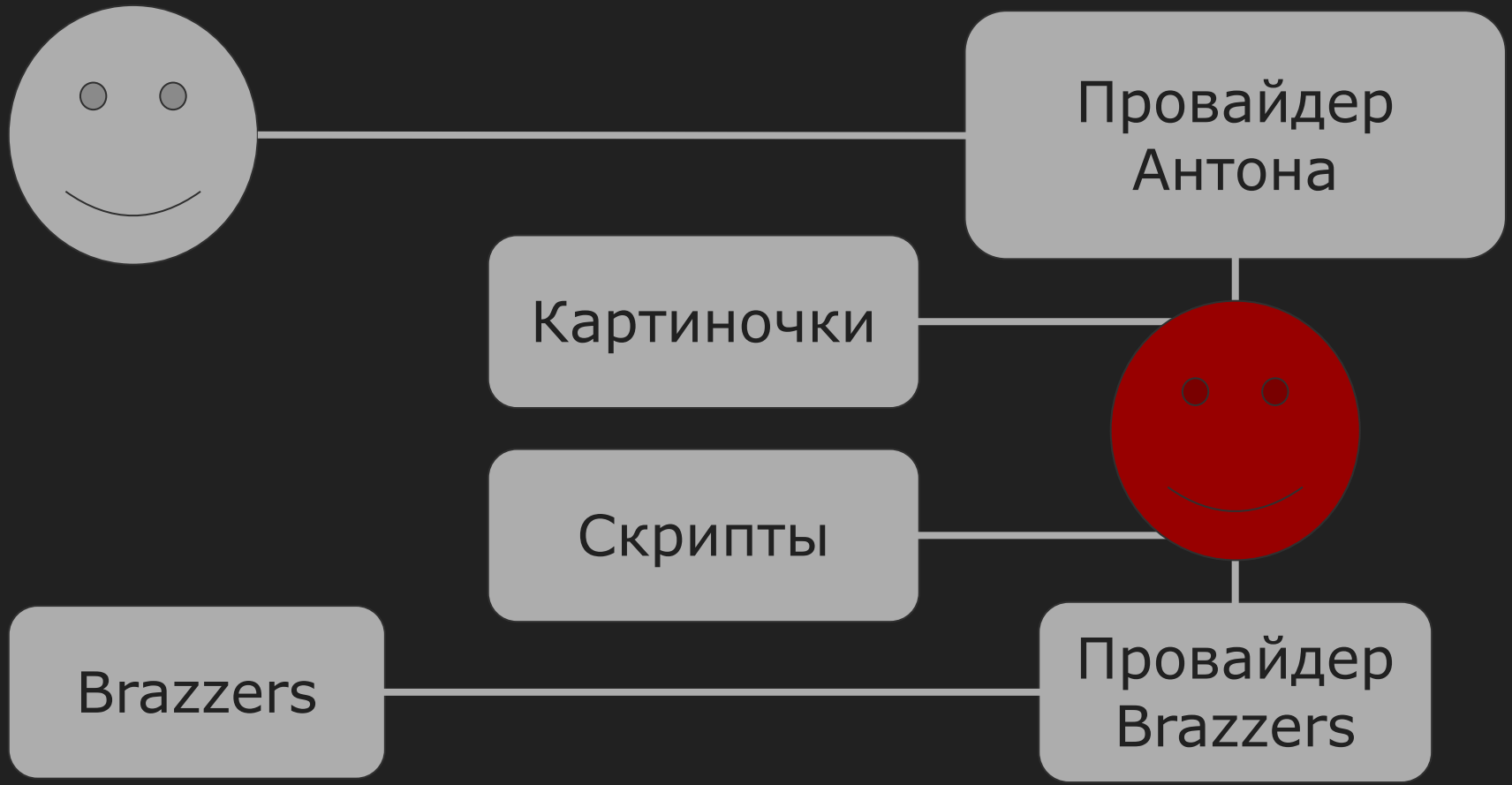

Провайдер Антона
Картиночки
Скрипты
Brazzers
Провайдер Brazzers


Провайдер
Антона
Картиночки
Скрипты
Brazzers
Провайдер
Brazzers


Провайдер Антона
Картиночки
Скрипты
Brazzers
Провайдер Brazzers


Провайдер
Антона
Картиночки
Скрипты
Brazzers
Провайдер
Brazzers


Провайдер
Антона
Картиночки
Скрипты
Brazzers
Провайдер
Brazzers


Провайдер Антона
Картиночки
Скрипты
Brazzers
Провайдер Brazzers

Это был XSS через MiTM

XSS — Это внедрение на страницу сайта вредоносного клиентского кода

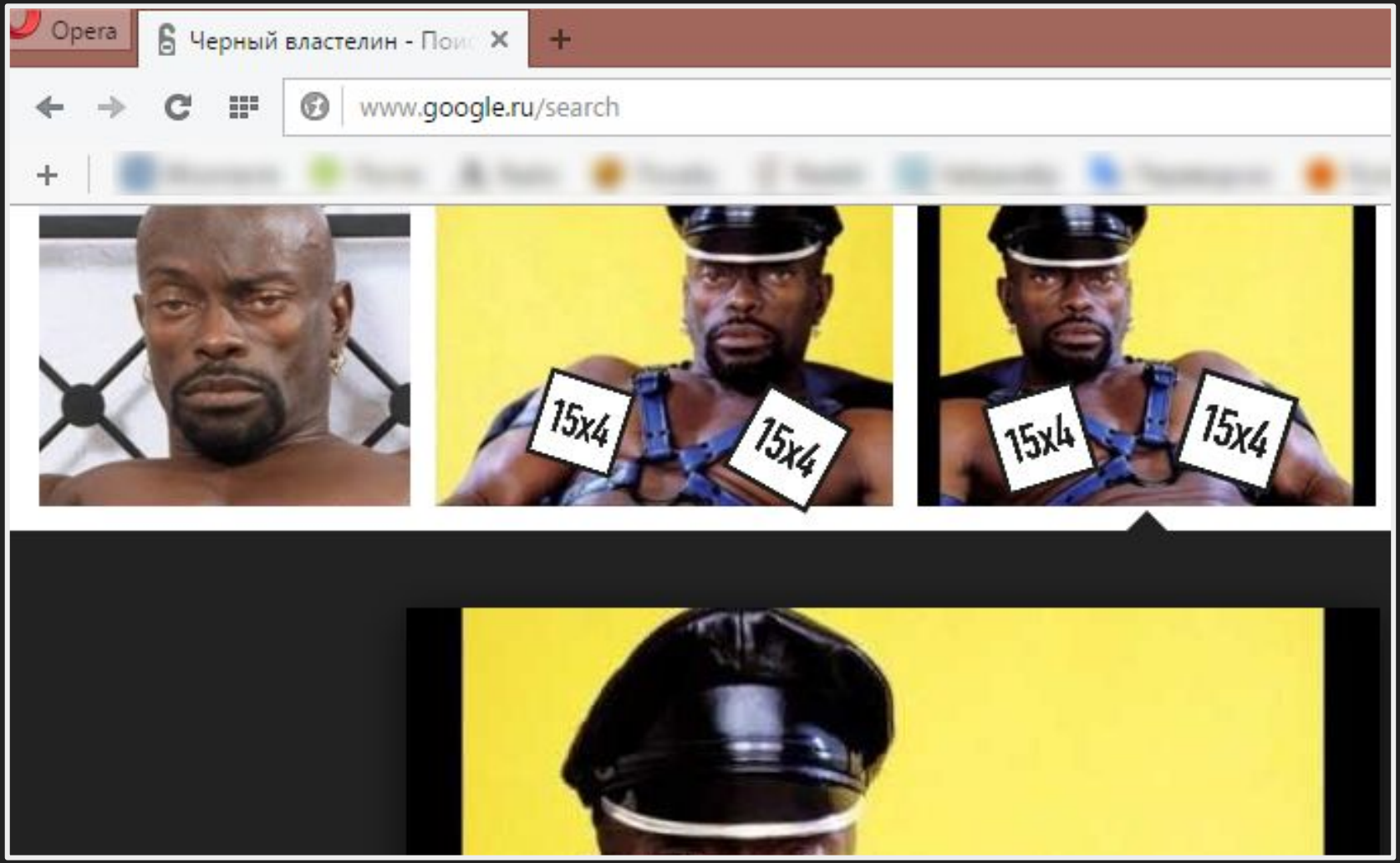
Opera

Черный властелин - Пои

www.google.ru/search

Черный властелин

Все | Картинки | Видео | Новости | Карты | Ещё | Настройки


Opera
Черный властелин - Пои
www.google.ru/search
15x4
15x4
15x4
15x4

¯_(ツ)_/¯

Кстати, про XSS

Промышленный шпионаж

от 400 000 руб / 1шт

2.56 BTC

Санкт-Петербург

Промышленный шпионаж

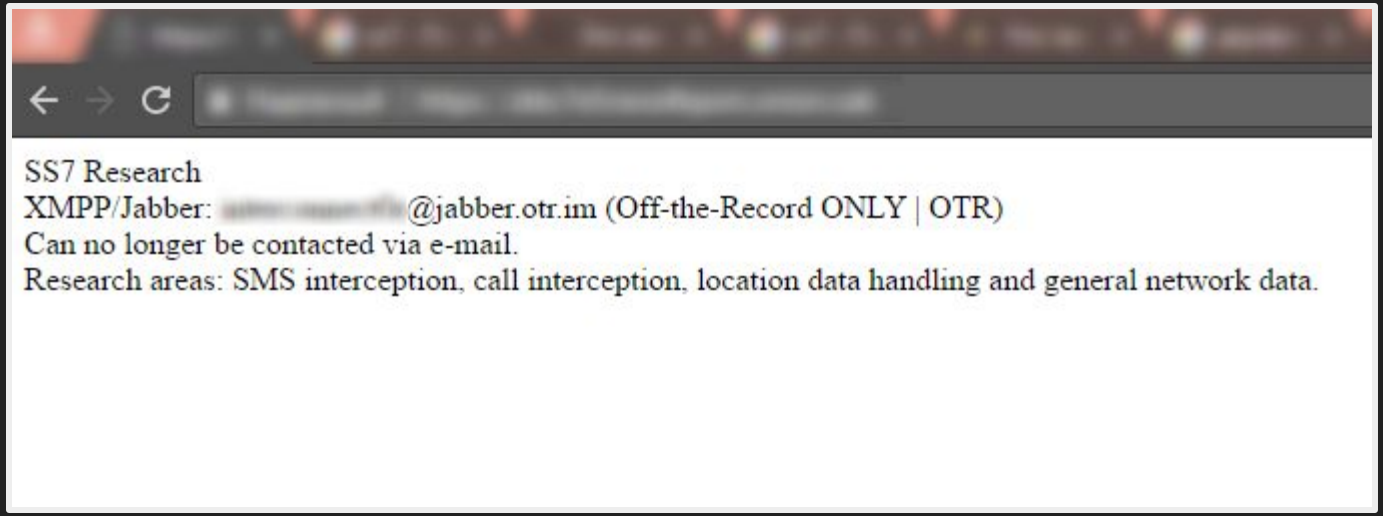
Предлагаем услуги по взлому сетей и получению конфиденциальной информации:

- Взлом беспроводных сетей;
- В случае наличия доступа к сети организация аттак MITM для перехвата учетных данных и паролей;
- Сканированние сети на наличие уязвимостей и их дальнейшая эксплуатация;
- Социальная инженерия;
- Иные вопросы связанные с безопасностью эксплуатации компьютерных сетей.

Цены

Цена зависит от конкретной задачи и объема работ, а так же от дополнительных затрат. В каждом отдельном случае сначала надо описать ситуацию и желаемый результат, менеджер сообщит вам стоимость работ. Ниже приведены приблизительные цены:

- Взлом Wi-Fi - от 200 000 р.
- Поиск и эксплуатация уязвимостей - от 700 000 р.
- MITM - от 300 000 р.
- Социальная инженирия - от 300 000 р.


SS7 Research
XMPP/Jabber: [redacted]@jabber.otr.im (Off-the-Record ONLY | OTR)
Can no longer be contacted via e-mail.
Research areas: SMS interception, call interception, location data handling and general network data.

Расходы расчетного периода

Сетевой ресурс **79153444450** Номер SIM карты /Виртуальный номер: [redacted]

Тарифные планы:

Москва - MAXI (MACC) (SCP) 01.04.2016 - 30.04.2016

Израсходованная сумма: **руб.**

Обслуживание:

Вам звонили!	01.04.2016 - 30.04.2016	22,8810
Все, что нужно 900	01.04.2016 - 30.04.2016	864,4080
СуперБИТ (042015)	27.04.2016 - 26.05.2016	296,6102
Черный список	01.04.2016 - 30.04.2016	38,1360
Детализация разговоров за период (на бумажном носителе)	30.04.2016 16:44:53	5,0847
Детализированный счёт, за сутки (через Интернет-Помощник)	30.04.2016 5:01:40	0,0000
Доступ без настроек: Добавление услуги	29.04.2016 8:11:50	0,0000
Доступ без настроек: Удаление услуги	29.04.2016 2:23:47	0,0000
Запрет информирования при добавлении/удалении услуг: Добавление услуги	29.04.2016 2:23:20	0,0000
Мобильный Интернет: Добавление услуги	29.04.2016 8:11:50	0,0000
Мобильный Интернет: Удаление услуги	29.04.2016 2:23:47	0,0000
Служба коротких сообщений: Добавление услуги	29.04.2016 8:11:50	0,0000
Служба коротких сообщений: Удаление услуги	29.04.2016 2:23:47	0,0000
Принудительная блокировка по неоплате счета	с 25.04.2016 11:29:43 по 28.04.2016 8:35:43	

Израсходованная сумма:

		руб.
Обслуживание:		
Вам звонили!	01.04.2016 - 30.04.2016	22,8810
Ежемесячная плата Smart	04.04.2016 - 03.05.2016	381,3559
SMS информирование при добавлении/удалении услуг: Удаление услуги	29.04.2016 2:25:14	0,0000
Доступ без настроек: Добавление услуги	29.04.2016 4:55:34	0,0000
Доступ без настроек: Добавление услуги	29.04.2016 18:52:18	0,0000
Доступ без настроек: Удаление услуги	29.04.2016 2:25:48	0,0000
Доступ без настроек: Удаление услуги	29.04.2016 18:45:08	0,0000
Замена SIM-карты	21.04.2016 20:07:47	0,0000
Запрет информирования при добавлении/удалении услуг: Добавление услуги	29.04.2016 2:25:14	0,0000
Мобильный Интернет: Добавление услуги	29.04.2016 4:55:34	0,0000
Мобильный Интернет: Добавление услуги	29.04.2016 18:52:18	0,0000
Мобильный Интернет: Удаление услуги	29.04.2016 2:25:48	0,0000
Мобильный Интернет: Удаление услуги	29.04.2016 18:45:08	0,0000
Служба коротких сообщений: Добавление услуги	29.04.2016 4:55:34	0,0000
Служба коротких сообщений: Удаление услуги	29.04.2016 2:25:48	0,0000
Состоявшиеся разговоры по 30.04.2016:		
SMS. Исходящее (Междугородная)	2 факт	6,4406
Итого		410,6775

- Свои устройства
- Зеленый замочек
- 2 Factor Authentication
- Бесплатный Wi-Fi?