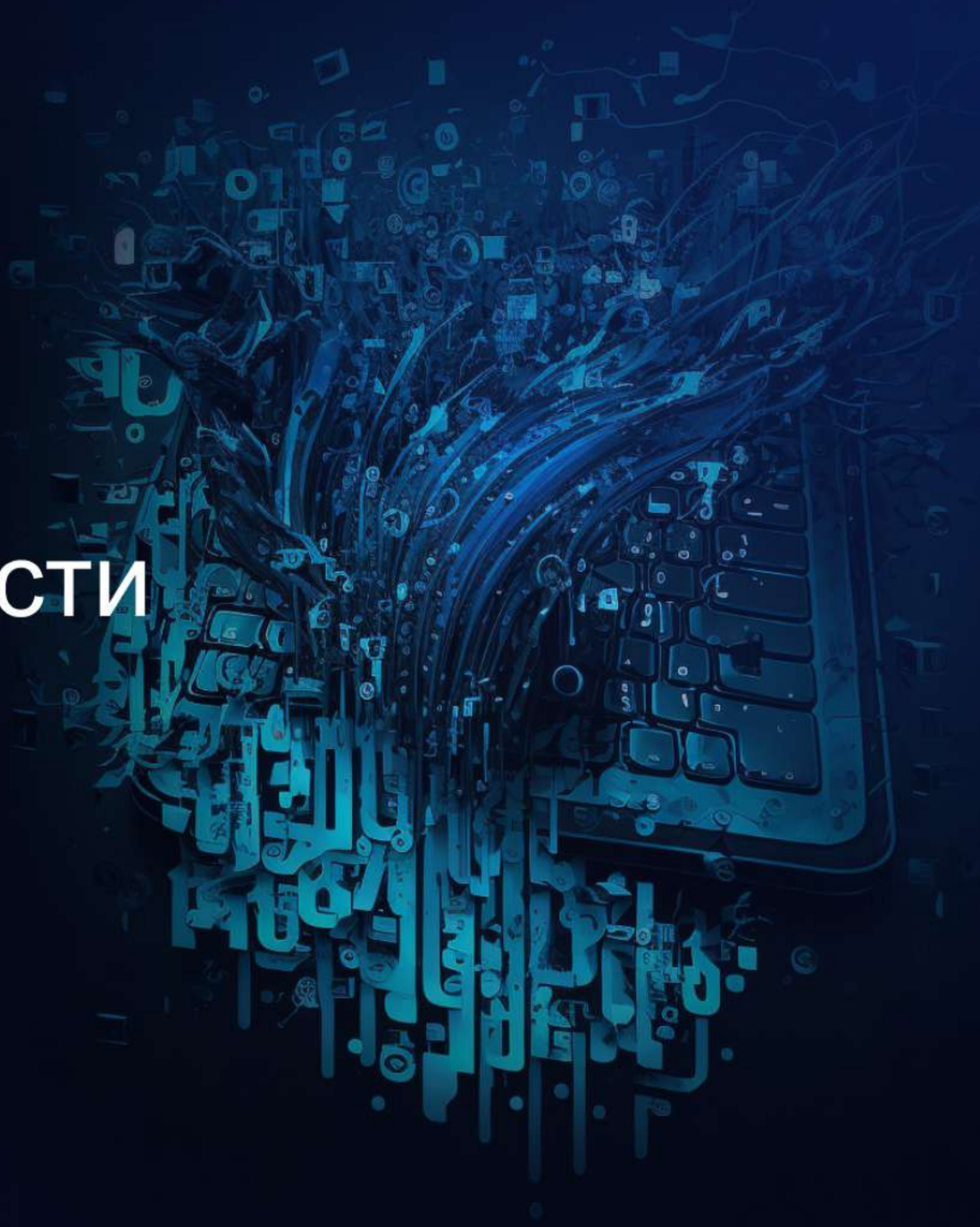
KillBot

Экран для защиты сайта



Цифровая идентификация личности

Григорий Мельников

Создатель KillBot

Елена Гурина

Доцент ММФ ТГУ

Google о нас знает всё, но и провайдеры не отстают

- В США в 2017 году был принят закон, разрешающий интернет провайдерам продавать историю посещений пользователей без их разрешения.
- В России аналог этого закона: "закон Яровой", провайдеры обязаны собирать и хранить данные о посещаемых сайтах и онлайн-активности.

Данные, к которым имеют доступ провайдеры, ограничены названием домена сайта, который мы посещаем: внутренние страницы и что именно мы там делаем недоступны при использовании закрытого HTTPS протокола.

KillBot Group

Цифровой след: кто и как собирает нашу историю просмотров

Собирают данные:

- **Скрипты аналитики:** Facebook Pixel, Google Analytics, Яндекс.Метрика и другие.
- **Сервисы защиты:** например, Cloudflare.
- **Браузерные расширения:** такие как Stylish.
- **VPN-сервисы:** такие как Freegate.

KillBot Group

Доступ к агрегируемым пользовательским данным

Компания SimilarWeb собирает данные у:

- Сторонних браузерных расширений;
- DNS-серверов;
- Своих браузерных расширений;

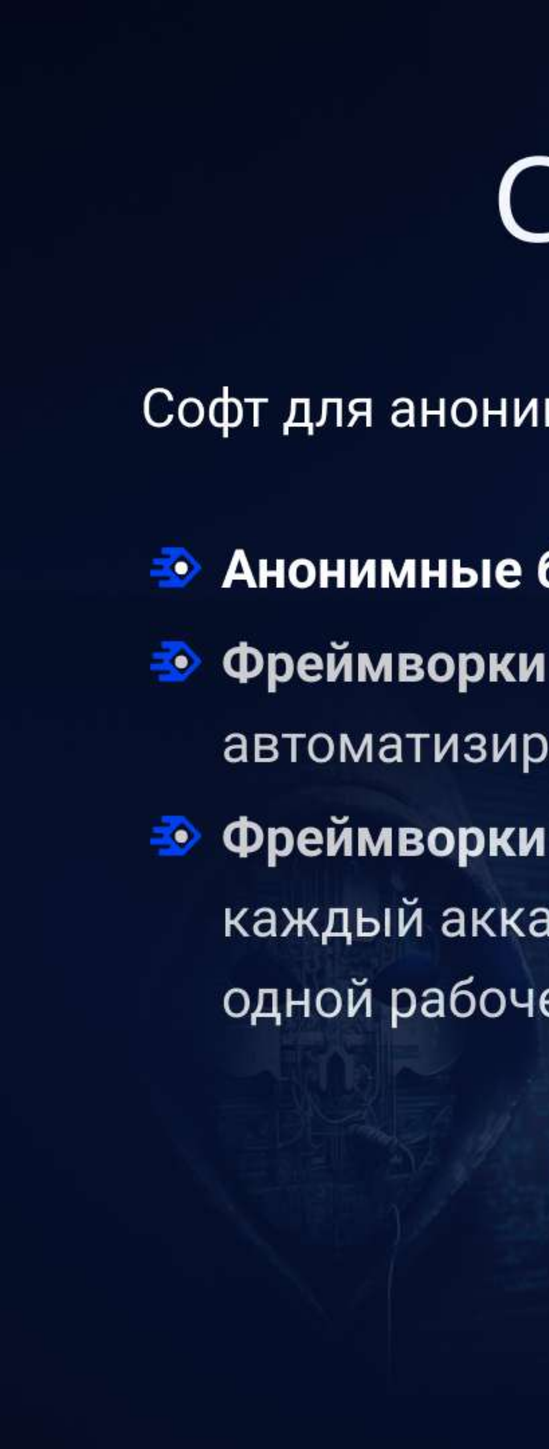
SimilarWeb предлагает продукт, который они называют «сервисом аналитики», а по факту - это скрытая торговля цифровыми следами миллионов людей.

KillBot Group

Софт для скрытия личности

Софт для анонимизации можно разделить на следующие категории:

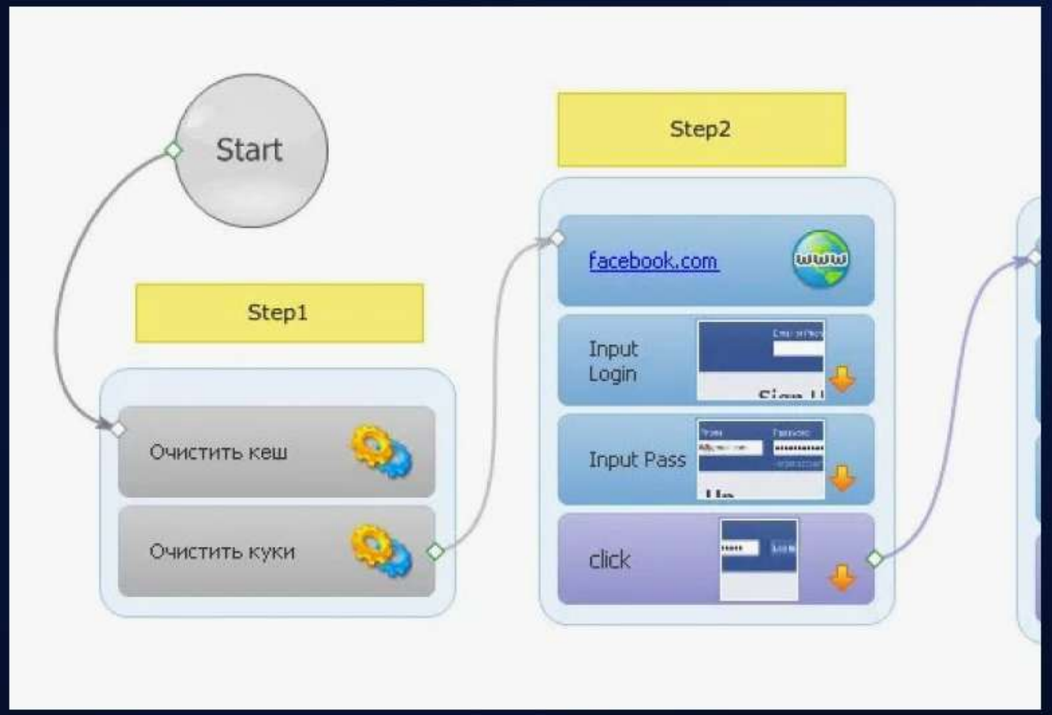
- **Анонимные браузеры типа TOP** для личного использования;
- **Фреймворки для создания ботов:** такие как BAS, Zennoposter создают множество автоматизированных цифровых пользователей;
- **Фреймворки мульти-аккаунтов с ручным управлением:** такие как MoreLogin, каждый аккаунт работает на удаленном реальном устройстве, администрирование с одной рабочей станции;



KillBot Group

Бота создать может каждый!

Боты обрели промышленные масштабы, когда появились удобные фреймворки для их создания. Чтобы создать бота уметь программировать не требуется.



ot Group

Резкий рост цены биткоина [бот Willy]

Рост с 150$ до 1000$ за биткоин обеспечили боты в течении нескольких месяцев в 2013 году.

Биржа Mt. Gox, искусственно увеличивала объёмы и поднимала цену биткоина через ботов. Эти факты подтверждаются внутренними логами, а также были признаны её бывшим генеральным директором Марком Карпелесом.

Источник: Fraudulent Trading Drove Bitcoin's $150-to-$1,000 Rise in 2013
https://www.investopedia.com/news/bots-drove-bitcoins-150to1000-rise-2013-paper/

KillBot Group

NVIDIA GeForce RTX 3090

Более 22 000 000$ заработали спекулянты на перепродаже NVIDIA GeForce RTX 30 серий. В день релиза 24 сентября 2021 года вся партия была выкуплена в течение нескольких секунд после начала продажи. Через несколько минут на eBay появилось множество предложений с ценой в более чем в 2.5 раза превышающую реальную.

Источник: Nvidia GeForce RTX 30 series scalping generates over US$22 million in sales via eBay as AMD's Big Navi GPUs and Zen 3 CPUs also fall victim to profiteering
https://www.notebookcheck.net/Nvidia-GeForce-RTX-30-series-scalping-generates-over-US-22-million-in-sales-via-eBay-as-AMD-s-Big-Navi-GPUs-and-Zen-3-CPUs-also-fall-victim-to-profiteering.509398.0.html

KillBot Group

GOOGLE - Ботнет Methbot

Более 7 000 000$ заработал на поддельных кликах Александр Жуков — российский хакер, создатель ботнета Methbot. В 2016 году его деятельность была разоблачена.

Источник: Russia's 'King Of Fraud' Gets 10-Year Prison Sentence In New York
https://www.rferl.org/a/russia-king-of-fraud/31556359.html

KillBot Group

Чем боты отличаются от реальных пользователей

- Нет истории навигации по интернету
- Нет связи пользователя с почтовым ящиком и другими устройствами
- Боты посещают одни и те же сайты
- Одинаковое время жизни ботов
- Отсутствие взаимодействия с "случайным" контентом
- Нет привязки к постоянному телефону
- Боты не платят

KillBot Group

KillBot

KillBot позволяет отличать посещения, совершенные бот-программами от действий реальных пользователей.

Для выявления ботов KillBot строит идентификаторы:

- Слепок браузера
- Идентификатор сети
- “Уникальный” UserID

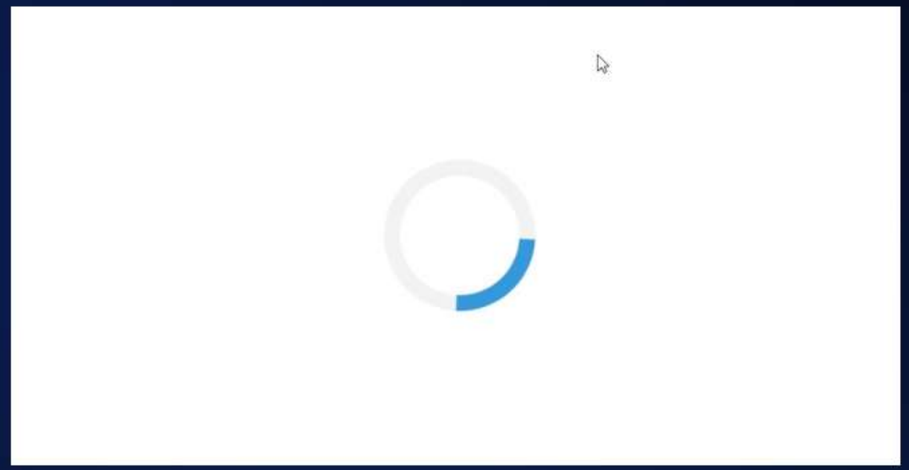
KillBot Group

Как с KillBot определить кто пользуется БОТ программой

- Заход бота оставляет слепок браузера
- Смотрим таблицу соответствия софта слепку браузера: какой именно софт в интернете оставляет такой же слепок
- По слепку мы определяем софт, который использовался для генерации бота
- Обращаемся к автору софта и берем список активных лицензий
- Владельцы лицензий на момент инцидента - это подозреваемые

KillBot Group

Бесплатный e-Mail не бесплатный



Для выявления личности пользователя, нужно проанализировать страницы сайтов, которые он посещает.

Что нужно сделать, чтобы распространить код, генерирующий UserID?

- Можно скупать популярные браузерные расширения (как делает SimilarWeb)
- Можно создать своё браузерное расширение и сделать популярным
- Популяризовать свой экран защиты сайта типу как у Cloudflare или у KillBot
- Создать свой бесплатный сервис аналитики, почтовый сервис и т.п.

Мы все пользуемся бесплатной почтой, бесплатной аналитикой. Оплата - это наша деанонимизация.

KillBot Group

Как будет выглядеть процесс идентифкации личности

- Провокация на переход по ссылке
- Получение уникального UserID
- Анализ страниц, которые посещает пользователь, IP адресов, выявление сервисов, которыми он пользуется
- Если пользователь платил, то нужно проанализировать источник платежа.
- Формирование круга лиц, кто с пользователем взаимодействовал.

KillBot Group

KillBot - лучшее решение на Amazon AWS по версии Uplify.APP

Кто использует KillBot:

- Uplify — агрегатор медийной рекламы (Бразилия и Индия)
- Elama — платформа, которая внедрила KillBot в свой маркетплейс инструментов.
- Маркетологи — для исключения ботов из показа рекламы.
- Владельцы сайтов — для защиты сайта от ботов.

Способы интеграции KillBot:

- API — используйте уникальные идентификаторы в своих решениях.
- DNS-прокси — подключение KillBot через сервер-посредник для защиты сайта.
- JS — как аналитический инструмент для сбора данных.

KillBot Group

Как сохранить анонимность?

- Нужно блокировать аналитические скрипты (например, Метрику и Аналитику)
- Не посещать сайты с экранами защиты (блокировать сервера этих сайтов)
- Не пользоваться анонимизирующими расширениями
- Не использовать другие браузерные расширения
- Использовать браузер типа TOR
- Использовать удаленный сервер для выхода в интернет (а не рабочий компьютер)
- Не вводить в формы свой логин, mail, телефон
- Не заходить на сайты которые вы обычно посещаете
- Не платить банковской картой и кошельками типа YooMoney
- При оплате криптовалютой — использовать миксеры
- Понимать что ты делаешь - если нет понимания, то этим можно не заниматься

KillBot Group

Обращайтесь!

KillBot:

- Григорий Мельников
- +7-913-817-92-98

Телеграм: https://t.me/grigoriy_melnikov

WhatsApp: https://wa.me/79138179298

Сайты:

https://KillBot-Group.ru/

https://KillBot.ru/ - личный кабинет

KillBot Group