УТРАТА АНОНИМНОСТИ В ВЕК РАЗВИТИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Меньшиков Ярослав Сергеевич
разработчик,
Net, ООО «ГисАвто»,
РФ, г. Новосибирск
E-mail: menshikov.yaroslav@gmail.com

Беляев Дмитрий Александрович
эксперт по ИБ, ООО «Секьюрити Бэнд»,
РФ, г. Москва
E-mail: da.belyaev@mail.ru

LOSS OF ANONYMITY IN THE AGE OF DEVELOPMENT OF DIGITAL TECHNOLOGIES

Yaroslav Menshikov
Net developer,
Net, LLC "GisAvto",
Russia, Novosibirsk

Dmitry Belyaev
Cybersecurity expert,
IS expert, Security Band LLC,
Russia, Moscow

АННОТАЦИЯ

В связи с развитием IT-технологий каждый человек испытывает потерю анонимности. Большинство людей не знает об этом. В статье объяснены множество факторов повлиявшие на заявленную проблему.

ABSTRACT

Due to the development of Tech, each person experiences a loss of anonymity. Most people do not know about this. The article explains many factors that influenced the stated problem.

Ключевые слова: анонимность, приватность, технологии, цифровой портрет, безопасность, кибербезопасность, наблюдение.

Keywords: anonymity, privacy, tech, digital portrait, security, cybersecurity, surveillance.

Целью данного исследования является акцентирование внимания к проблеме потери анонимности в наши дни. Сформулировать проблему – это первый шаг для всего общества к поиску решения проблемы.

Развитие IT-технологий испытывает ускорение в наши дни. Люди пользуются многими сервисами, предоставляя свои личные данные. Разработчики данных сервисов, получив ваши личные данные, начинают ими пользоваться в своих целях. Каждый человек пользуется не одной услугой, а множеством. Разработчики сервисов получают доступ ко многим вашим данным. Эти данные в совокупности представляют собой Ваш «цифровой портрет».

Самый простой пример использования цифровых портретов – это применение их третьими лицами для генерации адресной рекламы. Еще менее честные используют данные для генерации мошеннических писем. Мы живем в то время, когда цифровой анонимности практически нигде не учат, а компании умело пользуются этим фактом. Давайте перечислим часть актуальных сервисов, которые собирают информацию о пользователе.

1. *Ip-адрес*. Интернет-провайдеры годами хранят данные на каких ip-адресах работал их клиент. Это значит, что большинство ваших действий записываются в базы данных провайдера. Отчасти исправить эту проблему получается при использовании VPN-каналов.

2. *DNS-запросы*. При каждом обращении Вашего компьютера в сеть Интернет по имени хоста, а не по Ip-адресу (а это происходит практически каждый раз), например, google.com, операционная система запрашивает службу DNS, чтобы определить IP-адрес данного хоста. Провайдер, представляющий услугу DNS-записей, накапливает список тех сайтов, к которым происходило обращение и может предоставить их третьим лицам. Даже при использовании VPN следует обращать внимание какие DNS-сервера используются в системе.

Библиографическое описание: Меньшиков Я.С., Беляев Д.А. Утрата анонимности в век развития цифровых технологий // Universum: технические науки : электрон. научн. журн. 2021. 7(88). URL: *https://7universum.com/ru/tech/archive/item/12048*

3. *NFC-технологии*. Данную технологию используют устройства для выполнения бесконтактных платежей в магазинах. Технология использует радиочастотную идентификацию, а значит может использоваться для поиска устройства.

Пример: на входе в магазин установлена рамка, которая сканирует все имеющиеся при вас RFID-чипы: дебетовые или кредитные бесконтактные карты платежных систем, городские транспортные карты, рабочие карты доступа, даже некоторые ключи от машины. Эти данные легко собираются в базы данных и могут быть использованы для поиска людей.

4. *Беспроводные устройства вокруг нас*. Производители умных устройств (смартфоны, планшеты, детские часы с sim-картой и любые другие подобные устройства) закладывают функции поиска местоположения устройства для условий, когда GPS-функция выключена или недоступна. Это очень удобно, ведь данная технология позволяет успешно искать расположение устройства на картах yandex или google. Устройство сканирует Wi-Fi сети вокруг себя. В любой точке города ваше устройство видит набор таких сетей. Эти данные позволяют определить расположение с точностью до нескольких десятков метров. Данные о местоположении устройства отправляются на серверы третьих компаний.

5. *Использование публичных сетей Wi-Fi*. Достаточно иметь привычку подключаться к публичным wi-fi сетям чтобы стать жертвой хакеров. Хакеры используют специальные устройства способные вмешиваться в работу wi-fi точек доступа и вынуждающие Ваше устройство подключаться к их устройству, а не к публичной wi-fi точке доступа. Их целью является обманом заставить подключиться чтобы украсть учетные данные, номера банковских карт. В таких случаях передаваемые через эту сеть данные передаются через злоумышленника и становятся для него доступными. Для реализации данной задачи используется форма кибератаки Man-in-the-Middle.

6. *Tor/VPN*. Использование данных технологий не дает 100% гарантию анонимности. К текущему моменту разработаны методы деанонимизации зашифрованного трафика Tor. Совокупность посещаемых сайтов формирует уникальный цифровой портрет пользователя с точностью 96%. Ваш интернет-провайдер способен анализировать такие «отпечатки пальцев» и использовать эти данные для Вашей деанонимизации даже в условиях использования зашифрованных каналов связи.

7. *Современные смартфоны*. В некоторых фильмах показывали фантастические технологии, которые даже в выключенном телефоне продолжают работать и отправлять данные о расположении устройства для возможности поиска данного устройства. В наши дни на операционных системах Android, IOS используется технология Bluetooth Low-Energy, которая передает идентификационную информацию на ближайшие устройства. При этом неважно, включено Ваше устройство или выключено. Это дает способ определить Ваше месторасположение даже с выключенным телефоном при условии подключенного аккумулятора. В большинстве современных устройств аккумулятор является встроенным и не снимаемым элементом.

8. *IMEI - Идентификатор оборудования.* Идентификатор IMEI привязан к используемому устройству. Этот номер используется операторами мобильной связи и известен производителям оборудования. При каждом подключении устройства к мобильной сети происходит регистрация через сочетание IMEI и номера телефона в сотовой сети. IMEI используется некоторыми приложениями (часто банковскими программами), службами операционных систем Android и IOS для идентификации устройств. Использование номера телефона является отличным способом идентификации, не хуже предоставления паспорта. Ваш цифровой портрет становится лучшим подтверждением Вашей личности. Базы данных оператора мобильной связи хранят в том числе и другие данные: список мобильных антенн вокруг нас, насколько мощный сигнал устройства до каждой из этих антенн. С помощью триангуляции геолокации сигнала несложно рассчитывается подключенное устройство. Оператор видит и любые другие подключенные устройства. Устройства с похожими сигналами в один момент времени и подключенные к одним и тем же антеннам дают способ вычислить хозяина устройства.

Пример: человек носит с собой два телефона: один принадлежит ему, другой нет. Оператор мобильной связи легко определяет, у Вас чужой телефон.

Собираемая информация на основе IMEI может использоваться провайдером или другими третьими сторонами с доступом к этой информации для определения Вашего точного местоположения.

9. *Браузеры устройств*. При работе в сети Интернет браузеры получают уникальные данные (cookies) от любого сайта. Эти данные хранятся на Вашем устройстве. Таким образом веб-порталы точно знают кто зашел на сайт. На смену технологии cookies приходят технологии supercookies. Теперь провайдер помечает Ваши пакеты данных, и анонимность пользователя исчезает.

В совокупности данные cookies представляют собой уникальный набор данных. Некоторые вебпорталы научились определять пользователя без использования cookie, на основании используемых шрифтов, имени браузера, расширения экрана, операционной системы и других параметров.

10. *Банковские карты*. Банк автоматически собирает и накапливает информацию о всех наших покупках. Банк хранит стоимость покупки, тип товара, GPS-положение магазина на карте. Дополнительно банк знает Ваш возраст, пол, GPS-положение Вашего места жительства. На основании этих данных Банк рассчитывает Ваши предпочтения, предсказывает Ваши последующие действия проанализировав полученные данные. Эти данные анализируются автоматически, не используя труд людей. Далее автоматически банк определяет какую услугу и когда

Вам предложить. Эти данные банк может предоставлять третьим организациям.

Пример: на основании полученных данных банк видит где люди покупают аптечные препараты в некотором районе города. Если расстояние между местом проживания человека и аптекой становится относительном большим, то в данном районе есть проблемы с аптекой и, возможно, можно предложить партнерам банка открыть свою аптеку в этом районе.

11. *Голосовые службы устройств*. Данные службы в режиме постоянной работы анализируют местоположение устройства и звуки вокруг через микрофон. Речь идет о таких сервисах, как «Алиса», «Привет, Сири», «Окей Гугл». Микрофон Вашего устройства постоянно включен и производители голосовых служб записывают происходящее вокруг устройства. Что делают компании с этими данными? Кроме анализа фраз для поиска информации эти данные могут использоваться компанией для установления Ваших предпочтений, что может использоваться для создания адресной рекламы. Эти данные могут быть переданы третьим лицам для поиска Вашего местоположения.

12. *Использование антивируса/брандмауэра*. Брандмауэр антивируса анализирует сетевую активность устройства, работает с данными браузеров. Подобные программы имеют абсолютную власть на Вашем устройстве, не имеют преград для сбора любых данных и могут предоставлять удаленный доступ к устройству: файловый, веб-камера, микрофон, экран устройства.

Собранные данные в совокупности формируют Цифровой профиль человека. Данные этого профиля содержат в себе богатую информацию:

- Пол человека;
- Возраст человека;
- Семейное положение;
- Политические и религиозные взгляды;
- Финансовое состояние;
- Интересы;
- Привычки;
- Другие данные.

Согласно результатам исследования EFF (Electronic Frontier Foundation) [1], уникальность отпечатка браузера пользователя очень высока, и он содержит в себе ниже описанные данные:

- User-agent (включает версию браузера, версию операционной системы, тип устройства);
- Часовой пояс;
- Разрешение экрана и глубину цвета;
- Supercookies;
- Настройки куки;
- Системные шрифты;
- Список плагинов браузера с их версиями;
- Журнал посещений веб-сайтов;
- Другие данные.

Если говорить о статистике, то только раз на 286777 случаев случается полное совпадение отпечатков браузеров двух разных пользователей.

Согласно исследованию «Browser Fingerprinting via OS and Hardware Level Features» [2], точность идентификации пользователя при помощи отпечатка браузера составляет 99,24%.

Предложение решения проблемы. Сохранение анонимности сегодня – это практически невозможная задача для городского человека. Для сохранения анонимности в сети Интернет рекомендуется использовать решения, построенные на VPN-технологиях. В статье объяснено, что данное действие не является на 100% действенным, а значит для решения проблемы нужно повышать свой уровень знания цифровых технологий. По некоторым описанным в статье проблемам решением может быть только отказ от использования цифровых устройств.

Список литературы:

1. Electronic Frontier Foundation. How Unique Is Your Web Browser? Режим доступа: URL: https://coveryourtracks.eff.org/static/browser-uniqueness.pdf (дата обращения: 21.05.2021).
2. Researchgate. Browser Fingerprinting via OS and Hardware Level Features. Режим доступа: URL: https://www.researchgate.net/publication/316913422_Cross-Browser_Fingerprinting_via_OS_and_Hardware_Level_Features (дата обращения: 21.05.2021).