

Попов Юрий Леонидович,
Кандидат исторических наук,
ф. ВУНЦ ВВС «ВВА» в г. Челябинске,
Челябинск

Соловьев Иван Павлович, Студент,
ф. ВУНЦ ВВС «ВВА» в г. Челябинске,
Челябинск

Терёхин Матвей Евгеньевич, Студент,
ф. ВУНЦ ВВС «ВВА» в г. Челябинске,
Челябинск

Поляев Борислав Вадимович, Студент,
ф. ВУНЦ ВВС «ВВА» в г. Челябинске,
Челябинск

УТЕЧКА ИНФОРМАЦИИ ПОСРЕДСТВОМ ИСПОЛЬЗОВАНИЯ ЛИЦЕНЗИОННЫХ ПРИЛОЖЕНИЙ ИЗ МАРКЕТ ПЛЕЙСОВ

Аннотация: Рассматриваем пути и способы утечки информации, а также последствия утечки данных с устройств с расширенными мультимедийными функциями.

Ключевые слова: Утечка информации, маркет плейс, Pokemon Go.

С каждым годом количество пользователей мобильных телефонов и приложений значительно увеличивается. Современные смартфоны стали неотъемлемой частью нашей жизни, и с ними мы храним личные данные, фотографии, переписки и другую важную информацию. Однако вместе с удобством использования мобильных приложений возникает угроза утечки данных. В данной статье будет рассмотрена проблема утечки информации через приложения, загружаемые с маркет плейсов.

Многие пользователи не читают пользовательские соглашения и политики конфиденциальности при установке приложений. Часто в таких соглашениях прописаны права разработчиков на сбор и использование личной информации пользователей. Даже после появления новых правил, таких как GDPR (General Data Protection Regulation – Общий регламент по защите данных), пользователи по-прежнему часто соглашаются на условия, не осознавая возможных последствий. Это дает разработчикам возможность собирать данные о местоположении, контактной информации и даже содержанием переписок [1].

Компания Niantic, разработчик игры Pokemon Go, использовала данные игроков для создания «большой геопространственной модели» (Large Geospatial Model, LGM). LGM способна анализировать и интерпретировать физическое пространство. Она обучается на изображениях и данных, собранных в реальном мире.

Компания надеется, что LGM поможет роботам и нейросетям лучше ориентироваться в мире, а также выведет на новый уровень устройства дополненной и виртуальной реальности.

С момента запуска в 2016 году игра Pokemon Go завоевала миллионы поклонников по всему миру. Однако лишь недавно стало известно, что их активность помогла обучить искусственный интеллект. Как сообщает компания Niantic, разработчик игры, использует собранные данные для создания «большой геопространственной модели» (Large Geospatial Model, LGM). Нейросеть способна анализировать и интерпретировать физическое пространство.

Подобно тому, как большие языковые модели обрабатывают текст, LGM обучается на изображениях и данных, собранных в реальном мире. Благодаря этой технологии компьютеры



смогут не только понимать окружающую среду, но и взаимодействовать с ней. Это открывает перспективы для различных технологий: от дополненной реальности до робототехники и автономных систем. Niantic объясняет принцип работы модели через аналогию: представьте себя за церковью, которую модель «видела» только с фасадной стороны.

Эта технология базируется на платформе Lightship Visual Positioning System, которая позволяет закреплять виртуальные объекты в реальном мире с точностью до сантиметра. Одним из примеров использования является функция Pokemon Playgrounds. С ее помощью пользователи могут размещать покемонов в определенных местах, чтобы другие игроки могли с ними взаимодействовать.

На сегодня Niantic собрала более 10 миллионов изображений мест по всему миру, используя как данные из игр, так и сторонние приложения, например Scaniverse для 3D-сканирования объектов. Каждую неделю база данных пополняется миллионами новых снимков, сделанных от лица пешеходов. Это делает LGM уникальной, ведь большая часть данных других компаний фокусируется на дорогах и автомобильных маршрутах.

Авторы проекта отмечают, что люди очень хорошо ориентируются в реальном мире, что позволяет им прокладывать маршруты с учётом ландшафта, узнавать локации по фотографиям и находить дорогу до места, в котором были всего один раз в жизни. Если человеку показать фотографию объекта с двух ракурсов, то он сразу поймёт, что это один и тот же объект.

Нейросети не могут похвастаться такими возможностями из-за того, что они не знают, как выглядит физический мир и из чего он состоит. Инженеры Niantic начали решать эту проблему и разработали нейросеть MicKey. Она может сравнивать объекты, искать в них закономерности и понимать, что ей показывают один и тот же объект, но под разными углами. В некоторых задачах нейросеть справляется даже быстрее человека.

MicKey нужно много данных для обучения, чтобы она могла работать ещё лучше и быстрее. Оказалось, что игроки Pokemon Go собирали необходимые данные на протяжении восьми лет. У Niantic есть фотографии множества достопримечательностей, зданий и улиц по всему миру. К тому же, это не просто одиночные снимки, а фотографии с привязкой ко времени года и сезону. Всё это будут использовать для обучения большой геопространственной модели.

Исследователи компании отмечают, что Niantic сейчас – единственная компания в мире с таким датасетом. Ни у одной организации в мире нет такого количества снимков объектов физического мира с разных ракурсов. Также они подчёркивают, что объекты меняют свой облик на протяжении года.

Компания надеется, что её большая геопространственная модель поможет роботам и нейросетям лучше ориентироваться в мире. Например, с её помощью роботы смогут оперировать не точками на карте, а реальными объектами.

Когда ловцов монстров стало слишком много, представители власти и силовых ведомств стали пугать штрафами за ловлю покемонов в Кремле и в госучреждениях, а некоторые чиновники выдвинули предложения о запрете игры. Ещё они стали давать комментарии, в которых намекали на то, что игра может быть создана для слежки. Чаще всего СМИ цитируют отставного генерала-майора ФСБ Александра Михайлова:

«Кто и где покемонов ловит? » Если ребёнок – флаг им в руки, а если взрослые придурки играют на территории воинских частей, на режимных объектах – это проблема. Информация с этих мест уходит, а дальше уже дело техники.

Нельзя ведь сказать, что тот же чиновник и военнослужащий обязательно станет использовать игру у себя на работе. Но шанс такой есть, и, скорее всего, спецслужбы в разработке участия не принимали. Но вряд ли они пройдут мимо такой возможности по сбору данных.



Вскоре в сети стали появляться статьи с аргументами, подкрепляющими теорию о том, что игра создана для нужд разведки.

Niantic Labs (одна из трех компаний, которым принадлежит Pokemon Go) – детище Google.

Google была создана при активной поддержке ЦРУ. Запрет на использование этого поисковика чиновниками в служебных целях наложен не просто так.

Джон Хенк (на фото), глава Niantic Labs ранее прославился как создатель Keyhole, системы для глобального картографирования местности, позже купленной Google.

Keyhole спонсировал In-Q-Tel, созданный ЦРУ. Джордж Тенет, который возглавлял американскую разведку в то время (1997) даже дал официальный комментарий по случаю создания фонда:

В лицензионном соглашении написано, что игра может сливать собранную информацию государству, полиции и частным лицам:

Также настораживает список разрешений, которые требует игра. Несколько примеров того, на что просят позволения покемоны:

- сбор информации об аккаунтах пользователя (Google, Apple ID и т.д.);
- получение местоположение любыми способами (GPS, сотовая связь, Wi-Fi);
- считывание, удаление и запись файлов;
- вывод телефона из спящего режима;
- скачивание данных с интернета;
- доступ к bluetooth.
- просмотр информации о Wi-Fi соединениях.

Многие спецобъекты находятся неподалеку от населенных пунктов. И вокруг них гуляют дети и подростки. Их смартфоны могут [2]:

- Фиксировать в каких местах сигнал GPS пропадает или искажается.
- Компоновать оптимальные пути прохода на секретные объекты в GPS-треки (координаты могут вычисляться не по сигналу, а с помощью компаса и шагомера (например: 100 м на восток = плюс 0.001 градус к долготе)).
- Снимать номера автомобилей и лица людей, которые подъезжают к закрытым территориям.
- Записывать на видео дефекты в ограждениях, которые можно использовать для проникновения спецтехники.

Собранная информация может быть направлена в разные источники [3]:

1. Рекламные сети для целей таргетированной рекламы.
2. Аналитические компании, использующие данные для исследования рынка.
3. Мошеннические группы, которые могут использовать личные данные для кражи личных средств или шантажа.
4. Координаты могут быть переданы третьим лицам для использования в коммерческих целях.

И может привести к [4]:

1. Краже личных данных и средств.
2. Потери репутации и доверия к компании или разработчику.
3. Уголовным делам, если данные попадают в руки мошенников.
4. Психологическим проблемам пользователей, связанным с утратой контроля над личной информацией.

Утечка информации с мобильных телефонов через приложения становится серьезной проблемой в современном мире. Неосознанное согласие на пользовательские соглашения и



использование ненадежных приложений создают высокие риски для безопасности личных данных. Образование пользователей и информирование о возможных последствиях утечек информации являются необходимыми мерами для снижения рисков.

Список литературы:

1. Петров, И. А. Мобильные технологии и безопасность данных. Москва: Издательство "Наука", 2021.
2. Смирнов, В. Н. Конфиденциальность и защита данных в эпоху цифровизации. Санкт-Петербург: РГПУ им. Герцена, 2022.
3. Иванов, А. М. Безопасность мобильного контента. Новосибирск: Сибирское университетское издательство, 2020.
4. Кузнецова, Т. В. Риски использования мобильных приложений. Казань: Издательство "ТИС", 2019.

