Приложение 2

Как украинские спецслужбы вербуют россиян через интернет-квесты

Не всегда игра — это просто игра. Доверчивые пользователи уверены, что играют в игру, а на самом деле помогают врагу. Пока российская армия ведёт боевые действия с противником на реальном фронте, украинские спецслужбы активно «воюют» в виртуальном пространстве. Тихая, но коварная работа по вербовке россиян и добыче разведданных развернулась в защищённой, казалось бы, сети Telegram.

«С украинской стороны сейчас делается большая ставка на внутреннюю дестабилизацию России и теракты на нашей территории, в связи с чем схемы вовлечения российских граждан в противоправную деятельность достаточно изощрены», — сообщают правоохранители. Схема деятельности врага следующая: сотрудники украинских спецслужб создают в сети Telegram каналы, маскирующиеся под OSINT-проекты (англ. Open source intelligence), которые занимаются сбором данных из открытых источников. Пользователи вовлекаются в игровые задания, под прикрытием которых ведётся сбор разведданных о российской «оборонке» и вербовка пользователей.

Напомним: в последнее время правоохранители всё чаще выявляют граждан, занимающихся шпионажем по заданию украинских спецслужб. Подобные действия, напомнили в полиции, попадают под статью 276 УК РФ и предусматривают лишение свободы сроком от 10 до 20 лет.

Как работают иностранные агенты и каким образом пользователи попадают в хитро расставленные ловушки противника? Что за OSINT такой?

Механизм работы украинских спецслужб, на самом деле, давно известный, но, к сожалению, часто не заметный невнимательному или неопытному пользователю. OSINT-проекты – это только один из способов существующей разведдеятельности. Их цель – сбор информации из открытых источников в игровой форме. Пользователь отвечает вроде бы на обычные вопросы и незаметно для себя раскрывает личную информацию. Вражеские аналитики потом всю эту информацию консолидируют и составляют портрет человека. Дальше к работе подключаются психологи, которые, основываясь на полученной информации, уже начинают вербовать человека.

Чаще всего такой сбор информации маскируется под обычные квесты, когда пользователям предлагается зайти на какие-то ресурсы, найти определённую информацию, отгадать загадки и собрать ключи и т.д. Игровой формат сбивает пользователей с толку, они думают, что это безобидно, и даже не перепроверяют полученную информацию. Люди думают, что они выполняют интересные задания, цифровой квест, а на самом деле собирают информацию для недружественных организаций.

Ещё один распространённый метод разведки и вербовки молодёжи вражескими спецслужбами — так называемые игры ARG (Alternative Reality Games). В них задания тоже даются в интернете, а вот игровой платформой становится реальный мир.

Несмотря на то, что всё происходящее преподносится как игра, в ней используются реальные номера телефонов, локации, даже вознаграждение победителю. Всё это очень похоже на городской квест, только участники до конца толком не понимают, в чём участвуют, и не знают ничего об организаторах, поясняют эксперты по цифровой безопасности.

Поначалу игрокам даются простые и как будто безобидные здания – например, сфотографироваться рядом с определённым зданием в городе или объектом оборонного комплекса и передать снимок организаторам. По сути же, так участник неосознанно совершает преступление. После этого манипулировать им можно с помощью угроз и шантажа, а задания становятся, по сути, диверсиями.

Неспроста площадкой для своей деятельности иностранные спецслужбы выбрали Telegram. За годы существования сети у неё сложилась репутация надёжного ресурса с системой шифрования и верификацией каналов. В итоге у людей складывается ложное ощущение безопасности. Каналы для вербовки в Telegram зачастую имеют галочку верификации, которая на самом деле не требует подтверждения. Например, во «Вконтакте» каналу подтвердить свою официальность нужно через портал госуслуг. Для того чтобы получить такую галочку в Telegram, необходимо её просто оплатить.

Интернет помнит всё

К слову, подобные игровые методы сбора информации активно используются и в популярных соцсетях, правда, с более безобидной целью – для настройки таргетированной рекламы. Однако специалисты призывают пользователей быть осмотрительнее и выкладывать даже в соцсетях только тот контент, которым они готовы сейчас или когда-либо в будущем поделиться с миром. В противном случае всё, что хоть раз было оцифровано, может быть использовано против вас.

С точки зрения информационной безопасности использование соцсетей в принципе очень опасно. Если у человека открытый профиль, то по нему определённые люди могут узнать о человеке всё, что им нужно, и воспользоваться этим. Например, человек выкладывает фотографии мест, которые часто посещает, и люди понимают, где его можно встретить. Дальше на связь с ним выходит агент и начинает работу по вербовке».

Если российские сети в последнее время стали более щепетильны в отношении безопасности личной информации пользователей, то запрещённые в России интернет-площадки совершенно точно такой информацией делятся с иностранными спецслужбами.