Под колпаком у Большого Брата и его маленьких друзей

Admin • October 31, 2017

За нами следят со спутника — это реальность, а не выдумки параноика. Государство и бизнес хотят знать о каждом из нас всё и без остатка — разумеется, для нашей же безопасности и удобства. Но хорошо ли мы понимаем, чем придётся за это платить?

Недавно моего хорошего друга развели на деньги. Элегантно развели, с применением высоких технологий. К нему в скайп постучался отец, в разговоре назвал имена близких родственников, сказал, что находится в тяжёлой ситуации, и попросил на бедность денег — причём ровно ту сумму, которая лежала на банковской карте. Аккаунт, конечно же, был угнан вместе с почтовым ящиком. Друг недрогнувшей рукой перевёл остатки своей зарплаты неизвестному мошеннику на биткоины, платный аккаунт в тиндере и лёгкие наркотики.

И ведь это явно был не весёлый школьник. Чтобы украсть почту и скайп, много ума не надо — достаточно социальных технологий. А собрать прочие персональные данные? А получить доступ к балансу банковской карты? Причём надо понимать, что сбор такой информации «вручную» потребовал бы нечеловеческих усилий, и ради тех копеек, что им в итоге удалось надоить, такие вещи не затеваются.

Значит, где-то работает настоящий насос, тянущий информацию из соцсетей, где-то приобретаются закрытые данные о банковских счетах и некий алгоритм составляет из всего этого список готовых к обработке «лохов». Потом на него садится умелый копирайтер, который через украденные аккаунты рассылает «письма счастья». Даже если пять из десяти заподозрят подвох и пошлют «родственника» куда подальше — всё равно прибыль будет повыше, чем у иной китайской майнинговой фермы. А значит, тёмное будущее уже наступило.

Открой личико

Ладно, мы сами виноваты. Когда наши руки ещё только тянулись к новой игрушке по имени Facebook, умные люди ведь предупреждали, что не стоит выкладывать на всеобщее обозрение собственные фотографии, места работы, информацию о своём круге общения, хобби и адреса любимых кафе. «Да кому это может понадобиться», — весело отмахивались мы. «Мы не преступники, не террористы, не оппозиция, мы — маленькие люди и нам нечего скрывать». И выставили всё напоказ.

Десять лет спустя приватность в интернете умерла, а последний кол в её могилу забил появившийся прошлым летом сервис FindFace , задуманный как инструмент для спецслужб и до сих пор остающийся общедоступным в качестве «сервиса знакомств». Сфотографируй человека в метро и получи его страницу ВКонтакте на блюдечке. Первыми жертвами стали порноактрисы и эромодели, против которых «легион» имиджборда 2ch.ru развернул настоящую кампанию травли. Вторыми — участники митингов, которым не повезло попасть под объективы фотографов и камеры наблюдения.

Конечно, можно списать ужасы современного киберпанка лишь на собственную глупость, но проблема даже не в той информации, которую мы сами выложили в сеть, а в том, что мы позволили кому-то ещё ей бесконтрольно распоряжаться. В число допущенных к столу входят не только спецслужбы, но и корпорации, а следом за ними — и бизнес-структуры поменьше. Самая первая система всеобъемлющей слежки, слепившая в единый массив данных информацию из соцсетей, содержимое почтовых ящиков, содержимое смартфонов, историю поиска и данные геолокации, называлась Google. А предназначался весь этот «Скайнет» всего лишь для продажи таргетированной рекламы.

Главный принцип информационной безопасности гласит: «Чем больше баз данных и тех, кто имеет к ним доступ, — тем выше вероятность утечки». На общедоступный язык это переводится старинной немецкой поговоркой: «Что знают двое — знает и свинья». А тут даже не одна свинья, а целый свиноводческий совхоз, который давно пора закрыть за вопиющее несоответствие санитарным нормам.

«Тот, кто жертвует свободой ради спокойствия...»

На самом деле неизвестно, сколько терактов удалось предотвратить благодаря методам электронного наблюдения. Любая названная на официальном брифинге цифра может быть правдивой, а может быть и высосанной из пальца начальника пресс-службы. Зато мы знаем, что в мае этого года червь-вымогатель WannaCry заразил около 200 тысяч компьютеров по всему миру и только чудом не парализовал работу серверов МВД и систему управления РЖД. И что вылупился этот червячок из уязвимости, оставленной в Windows по требованию АНБ США для лёгкого доступа к содержимому компьютеров.

Неприятная правда заключается в том, что безопасность нескольких десятков потенциальных жертв несостоявшихся терактов мы обменяли на полное отсутствие бытовой безопасности для каждого. Кто написал ту нейросеть, которая прямо сейчас сортирует мои данные, — программист на государственной службе или мошенник? Кто смотрит на снимающую с себя топ девушку в раздевалке спортклуба — сервер системы наблюдения или пользователи «Двача», давно подключившиеся к этой камере? Кто загружает вашу фотографию в FindFace — тот, кто вчера постеснялся познакомиться в парке, или преступник, планирующий ограбить вашу квартиру?

Недаром Apple отказалась создавать для ФБР инструмент, способный обойти защиту iOS 8, — ровно по тем соображениям, что эта отмычка завтра может оказаться у кого угодно. Наследников Джобса и Возняка можно понять: они ещё толком не успели отмыть репутацию после массированного взлома iCloud, в результате которого хакерские блоги до сих пор пополняются фотографиями и видео с личных телефонов голливудских актрис и моделей. Представители закона в своей борьбе с Apple всерьёз рассчитывали на общественное мнение, но оно оказалось на стороне компании.

А в России население абсолютно равнодушно встретило как «закон Яровой», так и грядущий запрет анонимности в мессенджерах. Это притом, что история «социальных взломов» группы «Шалтай-Болтай» уже прогремела на всю медиасферу и любой читающий новости школьник знает, что даже чиновники Администрации президента не защищены от слива их интернет-переписки. Хранение же данных обычных пользователей, согласно новым законам, станет обязанностью операторов связи — «частных лавочек». А значит, уже

сейчас можно прикинуть масштабы грядущих утечек.

Внутри антиутопии

Сегодня статьи конституций всех стран мира, защищающие неприкосновенность частной жизни, уже можно считать юридическим нонсенсом. Но это только начало. Готовы ли мы к приходу «светлого завтра», в котором нам придётся обкладывать свою переписку непробиваемой криптографией, а выйти из дому можно будет только как в плохом шпионском боевике — нацепив парик и накладные усы?

Про усы, кстати, не шутка — в России уже разработан программный алгоритм, с помощью которого можно подобрать макияж, способный обмануть системы распознавания лиц. Который, в свою очередь, также может быть использован злоумышленниками. Так что хорошего выхода из этой ситуации нет и не предвидится. Либо государство ограничит собственные полномочия и запретительными мерами вернёт приватность на уровень начала 2000-х. Либо каждый из нас будет вынужден вырабатывать собственную стратегию выживания в условиях, когда доступ ко всей подноготной имеет не только Большой Брат, но и вообще кто угодно. Не всем хватит знаний и умений для того, чтобы вести свою маленькую кибервойну, а значит, мошенники голодными не останутся.

Оригинал