Как захлопнется цифровая западня.

14.03.2021

5 февраля на водоочистной станции города Олдсмар во Флориде был предотвращен биотеракт. Хакер удаленно проник в систему и поднял уровень щелочи в воде до опасных значений. Но оператор, заметив неладное на дисплее, вовремя исправил проблему, и в итоге люди не пострадали. А могли бы.

С небес на землю

Пока человечество следит за марсианским дебютом Perseverance, на Земле тихой сапой сбывается другая фантастика — отнюдь не космическая. И что ужасало отцов киберпанка, теперь радует обывателей.

Чтобы заказать такси или товар, купить билет, занять очередь или деньги, оформить любую услугу, сейчас достаточно пару раз стукнуть пальцем по экрану смартфона.

Камеры слежения, связанные с системой распознавания лиц, помогают ловить “преступников”.

“Хирурги” оперируют пациентов на расстоянии — руками роботов.

По дорогам колесят беспилотные машины, а дроны летают над грядками, следя за созреванием арбузов.

“Умный” дом избавляет от необходимости вставать с кровати для включения света, кормления рыбок или закрытия штор.

Всюду датчики: одни защищают от протечки труб, другие сообщают, где ваш ребенок, третьи сигнализируют о незваных гостях, пока вы в отпуске.

По меркам исторических масштабов все это пришло в нашу жизнь быстро — не успело и поколение смениться. Но ронять челюсть на пол от контраста между «до» и «после» мы почему-то не спешим. Это же не полет на Марс! Писатель-фантаст Брюс Стерлинг на страницах эссе «Будущее уже началось» верно подмечает:

«Киберпанк в середине 1980-х нес в себе наивно-лирическое утверждение невероятного: мир однажды станет таким… Когда же это время пришло, киберпанк никто не назвал пророческим, к нему относились как к клише. Он стал банальным и архаичным, так как его авторы возводили на пьедестал то, на что сейчас не обращают никакого внимания».

Почему так? Возможно, повышение комфорта за счет технологий мы принимаем как должное.

Нынешний век действительно очень удобен: свободного времени у нас гораздо больше, чем было у наших пап и мам в аналогичном возрасте. Но какой ценой?

Ответ на этот вопрос, помимо пророчеств о технических новшествах, предлагает все тот же киберпанк.

Алгоритмы, упрощающие жизнь, беспристрастны и точны, работают без устали, есть не просят — и тем не менее остаются уязвимыми. Их просто-напросто можно взломать и применить во вред.

Жизнь под прицелом

Хакеры — давно не новость. Еще с середины 1980-х они используют пробелы в цифровой защите компаний, чтобы сорвать куш. Недавно, если помните, досталось разработчикам Cyberpunk 2077, у которых злодеи потребовали выкуп за неразглашение похищенных данных.

А фишинг? Согласно отчетам Avito, «Тинькофф» и «Лаборатории Касперского», только в 2020 году интернет-мошенники украли у россиян 150 млрд рублей.

Сколько существует Глобальная сеть, столько ее и точат черви — вроде бы ничего необычного. Но повсеместная цифровизация последних лет создала почву для новой угрозы, куда более масштабной.

В 2018-м ООН приняла «Глобальную контртеррористическую стратегию», где есть такая фраза: «Террористы могут расширить свои возможности причинения вреда, используя растущую взаимозависимость между различными секторами, включая банковско-финансовый сектор, сектор телекоммуникаций и связи, службы экстренной помощи, воздушный, морской и железнодорожный транспорт, а также службы энерго- и водоснабжения, в целях проведения кибератак на соответствующие объекты критически важной инфраструктуры».

Как тут не вспомнить о недавней попытке биотеракта во Флориде? Или декабрь 2016 года, когда хакеры на два дня парализовали работу Министерства финансов и государственного казначейства Украины?

Под ударом находятся буквально все сферы дивного нового мира. Еще в 2014-м лаборатория IOActive показала, как можно удаленно взломать системы контроля трафика в США, Великобритании, Франции, Австралии, Китае и других странах: хакер просто захватил управление светофорами, словно герой популярной игры Watch Dogs.

С 2016 года то и дело происходят кибератаки против медицинских учреждений — в октябре 2020 года Министерство здравоохранения США, агентство CISA и ФБР заявили о беспрецедентной угрозе со стороны киберпреступников для американских больниц.

Несколько позже в журнале Nature вышла статья израильских ученых о том, что при помощи вредоносного ПО на лабораторных компьютерах биотеррористы могут чужими руками создавать опасные вирусы. Конечно, паника не обошла стороной и атомную энергетику.

Если думаете, что эти страсти кипят где-то далеко и вас не касаются, просто оглянитесь вокруг.

Как установили в прошлом году специалисты Tencent, программа под названием BadPower способна поджигать смартфоны на быстрой зарядке.

А особенно беззащитен так называемый интернет вещей, построенный на обмене данными между устройствами, в том числе компонентами умного дома. Их уязвимость обусловлена тем, что владельцы гаджетов зачастую оставляют нетронутыми заводские настройки и пароли.

Чем это чревато, показал в 2016 году ботнет Mirai.

Взяв под контроль множество смарт-камер, он провел с них DDoS-атаку на провайдера Dyn, в результате чего легли серверы Netflix, HBO, Amazon, PayPal, Visa, Reddit, Twitter, Spotify и других известных компаний.

Большой Брат смотрит

Для простого человека перечисленное выглядит как вторжение в частную жизнь неведомых и зловещих сил. Сидит где-то хакер и, ловко заметая следы, воздействует на устройства и службы, которыми мы пользуемся.

Но что если за вмешательством стоят вполне известные силы? Наверное, нет на свете производителя электроники, который не думал бы о дистанционном контроле.

В частности, гаджеты на базе Intel содержат Active Management Technology (или Intel ME) — инструмент, предназначенный для удаленного модерирования. Доступа к нему у рядового пользователя нет.

Компании применяют такие системы не только для отладки, но и для отключения некоторых функций без нашего ведома, как случилось, например, с «серыми» Smart TV Samsung в России.

Не все же читают лицензионные соглашения полностью — большинство жмет «Согласен» под стеной текста, чтобы как можно скорее воспользоваться услугой.

Иногда подобное случается со вполне серьезными структурами. В октябре 2019-го представители «Газпрома» заявили, что австрийские компрессоры LMF были отключены через спутник. По словам экспертов, это мог сделать производитель из-за истечения срока обслуживания или по причине санкций. Со своей стороны, госкорпорации тоже увлечены цифровым контролем.

Летом 2020 года «Ростех» и Фонд развития промышленности представили умные счетчики электроэнергии, способные автоматически передавать показания оператору и гасить свет за неуплату.

Вроде все по уму, но осадочек неприятный. Потому что в голове возникает пример страны, где такие решения возведены в культ.

Китай огромен и многолюден, но при этом необычайно консолидирован. Здесь вовсю применяется социальная инженерия с использованием смарт-устройств, сбора и обработки больших массивов данных.

Пример такого подхода — знаменитая «система социального кредита». Общественная польза человека в рамках этой системы оценивается автоматически, без участия людей, а обладатели низкого рейтинга ограничиваются в правах.

Причем дело только набирает обороты: сегодня камеры слежения умеют распознавать лица, а завтра они научатся выделять в толпе опасных личностей и применять к ним меры.

Военно-техническая корпорация China Electronics Technology Group совместно с компаниями из США и Европы уже ведет разработку такой технологии. В ее основе — распознавание движений и эмоций людей, склонных к совершению преступления.

То есть человек еще никого не ограбил, но компьютер на основе анализа массы архивных записей понимает, что ограбление вот-вот состоится, и сам обращается в полицию.

Помните фильм Спилберга «Особое мнение»*? Смешно сказать, в начале 2000-х он казался параноидальной фантазией из книг Франца Кафки. А теперь представьте, что доступ к этой или любой другой похожей системе получили настоящие, а не предполагаемые злодеи.

Что будет дальше?

Каждый хочет жить удобно и безопасно. С этой целью все больше задач возлагается на цифровую среду, которая, в свою очередь, остается уязвимой для манипуляций со злым умыслом. Мы сталкиваемся с типичным выбором из киберпанка: с одной стороны — высокие технологии, а с другой — низкий уровень жизни.

В романе «Виртуальный свет» классик жанра Уильям Гибсон описывает общины, ушедшие из-под контроля корпораций и компьютеров, даже телевизоры там запрещены.

Звучит благородно, хотя на деле мы видим нищих дикарей, построивших свою диктатуру с железным занавесом в ответ на диктатуру глобальных технологий.

Увы, фантасты лишь описали цифровую западню, не предложив адекватного способа избежать ее. Но если он существует, его необходимо найти.

Александр Бурсов

**американский научно-фантастический фильм Стивена Спилберга по мотивам одноимённого рассказа Филипа Киндреда Дика. Действие происходит в 2054 году в Вашингтоне. В стране внедрена система профилактики преступлений Precrime, благодаря которой число убийств удалось свести до нуля. Система на основе анализа данных «видит» преступления, которые будут совершены в ближайшем будущем и выдаёт на экран имена убийцы, жертвы, время убийства и тип преступления (преднамеренное или непреднамеренное). Несостоявшихся убийц помещают в анабиозные капсулы.*

Источник: https://rusvesna.su/news/1615714787