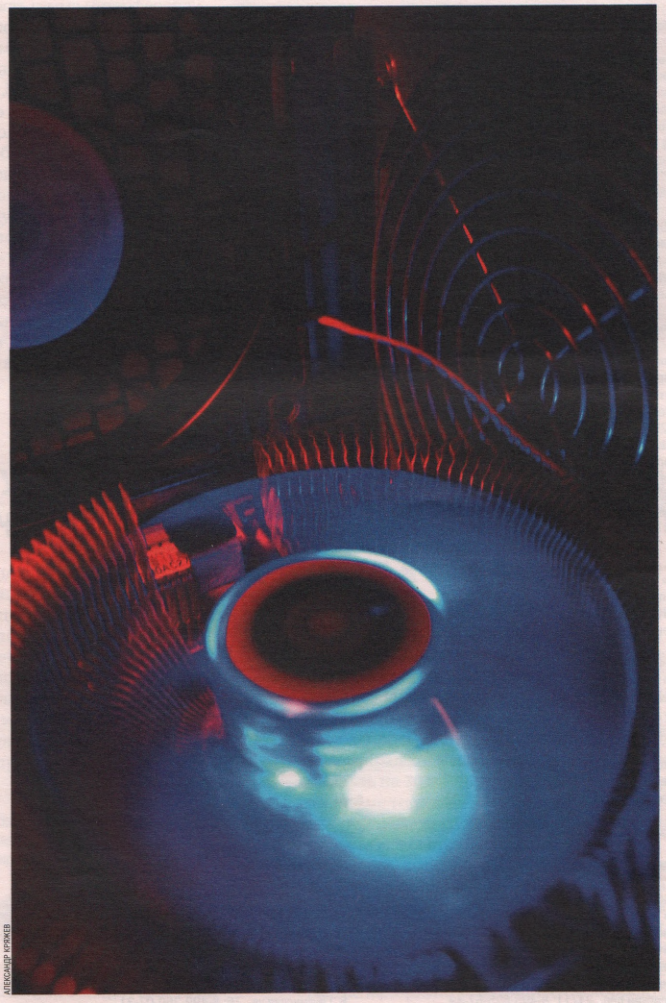
ПРЕДАЮЩИЕ УСТРОЙСТВА

НОВУЮ ЭРУ КИБЕРПРЕСТУПЛЕНИЙ ОТКРЫЛИ УМЕЛЬЦЫ ИЗ ИЗРАИЛЯ, ПОХИТИВ ДАННЫЕ С ОТКЛЮЧЕННОГО ОТ СЕТИ КОМПЬЮТЕРА. ДЛЯ ЭТОГО ВЗЛОМЩИКИ ВОСПОЛЬЗОВАЛИСЬ… ВЕНТИЛЯТОРОМ, КОТОРЫЙ ОХЛАЖДАЕТ КОРПУС МАШИНЫ ИЗНУТРИ. КАК СЕГОДНЯ ВЫЖИТЬ В ЦИФРОВОМ ПРОСТРАНСТВЕ И ЧЕГО НУЖНО ОПАСАТЬСЯ РЯДОВОМУ ПОЛЬЗОВАТЕЛЮ ГАДЖЕТОВ, УЗНАЛ «ОГОНЕК»

Елена Кудрявцева



АЛЕКСАНДР УРЯЖЕВ

Кто бы мог подумать, что мирный вентилятор может шпионить за хозяином?

Раз в год исследовательский центр SplashData публикует самые популярные пароли, которыми пользователи во всем мире защищают свои гаджеты. Уже много лет на первом месте оказывается нехитрая комбинация «password» и пароль «123456», которые используют сотни тысяч человек по всему миру. Собственно, для того чтобы привлечь внимание беспечных пользователей к проблеме киберпреступлений, ученые из Лаборатории компьютерной безопасности Университета Бен-Гуриона решили провести показательную кражу данных с отключенного от Сети компьютера. Для этого они использовали довольно редкий шпионский прием. Компьютерщики написали небольшую шпионскую программку Fansmitter, которая умеет делать несколько занятных вещей. Во-первых, она выбирает на компьютере нужный файл и считывает информацию, во-вторых, передает ее вовне в буквальном смысле по воздуху. Технология работает исходя из того, что вся информация в компьютере представлена либо единицей, либо нулем. Для того чтобы передать единичку, программа запускает на машине сложные вычисления и тем самым полностью загружает процессор, он нагревается — вентилятор шумит сильнее. Если крутится медленнее — программа передает ноль. Шум записывается на лежащий рядом смартфон и передается за пределы комнаты.

— Подобные шпионские способы передачи информации называют «нетрадиционными информационными каналами»,— рассказал «Огоньку» Дмитрий Кузнецов, директор по методологии и стандартизации компании Positive Technologies.— Сюда входят любые способы передачи данных через предметы, которые для подобной передачи не предназначены. Помните в фильме «Семнадцать мгновений весны» на окно ставили горшок, который обозначал, что все хорошо, а его отсутствие означало засаду? Это как раз была передача одного бита информации нетрадиционным способом. Сегодня такие возможности широко распространены в компьютерных технологиях и представляют собой некие «закладки» в вашем компьютере, наподобие программы Fansmitter, которые могут потихоньку передавать данные, когда нужно злоумышленнику.

В последние 2–3 года широким полем для деятельности хакеров стал «интернет вещей», то есть все гаджеты, которые работают дома и имеют выход в Сеть

Конечно, много информации таким способом не похитишь — в сутки можно получить максимум 1–2 килобита. На секретное донесение это не тянет, но вот ключ или шифр для доступа к важным компьютерным системам получить можно. Это становится особо интересно, учитывая, что вентиляторы есть на всех компьютерах, в том числе на тех, что работают на атомных электростанциях и различных военных объектах. Учитывая последствия вмешательства в столь опасные системы, возникает вопрос: возможно ли в принципе обезопасить компьютерные системы от утечек?

В России проблему нетрадиционных каналов передачи данных активно изучали в середине 2000-х. Тогда спецслужбы поставили перед учеными вопрос: существуют ли вообще такие каналы и стоит ли тратить силы на борьбу с ними? В итоге специалисты доказали, что подобные скрытые каналы действительно могут работать. Например, успешно прошел эксперимент, во время которого два человека, находясь в разных городах, смогли обменяться информацией, увеличивая или уменьшая количество пересылаемых сообщений по сети. Причем смысл сообщений был абсолютно не важен — важен был именно факт передачи. После чего был разработан государственный стандарт по информационной безопасности, который рассказывает о том, что такое скрытые каналы, и предлагает способы пресечения утечек. Правда, сегодня финансирование этого направления приостановлено, что, по мнению экспертов, ставит Россию в уязвимое положение.

— Вообще, работы по проникновению в компьютерные системы ведутся давно, в этих исследованиях заинтересованы правительства разных стран. В вооруженных силах организованы так называемые киберподразделения, которые действуют и как средство защиты, и как средство нападения,— рассказал «Огоньку» директор Института точной механики и вычислительной техники им. С.А. Лебедева РАН профессор Александр Князев.— Отметим, что область применения очень обширна, и скрытые каналы относятся к любой сфере нашей действительности. Так, эти каналы нашли применение в телевещании, со временем преобразовавшись в информацию по подписке заказчика и телетекст. Также их использовали для анализа прочности мостов, их пропускной способности. Новые протоколы появляются непрерывно, но многого мы не видим, поскольку не обладаем адек-

Детали

НА ВИДУ И НА СЛУХУ

ОКРУЖИВ СЕБЯ БОЛЬШИМ КОЛИЧЕСТВОМ ПОЛЕЗНЫХ ГАДЖЕТОВ, МЫ НЕ ЗАДУМЫВАЕМСЯ, ЧТО У НИХ ЕСТЬ СОБСТВЕННЫЕ ВИДЫ НА СВОИХ ХОЗЯЕВ

Большой брат

Многие телевизоры последнего поколения, имеющие выход в интернет, собирают информацию о том, каким каналам вы отдаете предпочтение, какие фильмы ищете в Сети и передачи какого содержания смотрите дольше всего. Помимо этого, умное устройство запомнит все фильмы, которые вы смотрели на нем с флешки. Собранную информацию он отсылает производителям, которые продают ее маркетологам и рекламодателям. Информация уходит без ведома самого телезрителя — номинально он соглашается с таким положением дел, подписывая пользовательское соглашение.

Чтобы понять, следит ли за вами собственный телевизор или нет, нужно проверить, есть ли у него активный исходящий трафик. Затем можно проследить, куда именно сливает информацию о ваших увлечениях ваш жидкокристаллический друг.

Глаз Саурона

Камера ноутбука может стать источником настоящих проблем для незадачливого пользователя. Через нее можно наладить видеотрансляцию из вашей квартиры прямо на экран хакера. При этом злоумышленник может запускать у вас на компьютере любые видеофайлы. Чтобы попасть в чужой компьютер, хакеры пользуются простыми программами, предназначенными для управления компьютером на расстоянии. Подключиться к вашей камере можно совершенно безнаказанно, если вы не заменили в заводских настройках пароль удаленного доступа к компьютеру.

Самые неприятные истории подглядывания через камеру связаны с шантажом молодых девушек: пират грозит выложить домашние видео в интернет, если те не будут делать откровенные фото и отсылать ему. Самое громкое дело по факту использования чужих камер случилось в 2014 году, когда на хакерском ресурсе одновременно разместили записи с нескольких тысяч каналов из США, Франции и Нидерландов.

Дороги, которые мы выбираем

Смартфон является прекрасным средством для сбора информации о своем владельце. В тот момент, когда пользователь включает устройство, чтобы найти нужную улицу, он и не думает о том, что телефон тщательно фиксирует не только все маршруты путешествий, аккуратно запоминая, где именно и в какой день вы ходили, но и отмечает, сколько времени вы провели в том или ином месте. Собранную информацию смартфон аккуратно передает компании, чьей сотовой связью вы пользуетесь, а также в 100 процентах случаев — производителям мобильных платформ. Те и другие продают данные рекламщикам. Благодаря этому симбиозу лично вы будете получать СМС-приглашения зайти в ресторан или в магазин одежды именно тогда, когда проезжаете мимо. Кроме этого, существующие в смартфонах функции «родительского контроля» позволяют точно определить ваше местонахождение в каждую секунду времени с другого телефона.

Попасться в сети

Социальные сети, без сомнения, основные накопители сведений о вашей жизни в интернете. Но даже если вы вдруг решите удалить страничку и все фотографии на ней, информация о ваших действиях в Сети все равно останется. О каждом вашем поисковом запросе и клике узнает провайдер, сайт, к которому вы обратились, те же соцсети (когда в конце статьи стоит кнопка для перехода в сеть, она автоматически отслеживает ваши интересы), особые системы анализа посещаемости и баннерные сети. Все это позволяет маркетологам составить ваш потребительский портрет, чтобы атаковать контекстной рекламой. Один из известных случаев такой атаки связан с работой американской сети интернет-магазинов Target, которая научилась вычислять, кто из ее покупательниц ждет ребенка. Для этого специалисты проанализировали данные о покупках женщин, уже родивших ребенка, и выяснили, что в первые недели беременности те закупали минеральные добавки и мыло без запаха. На основе этой информации маркетологи теперь выуживают клиенток и шлют им рекламу роддомов, мебели для новорожденных и ползунков задолго до того, как те, может быть, решились рассказать о своем интересном положении окружающим.

Чужая рука на пульсе

Фитнес-браслеты — относительно новый для большинства россиян гаджет. Продвинутые модели включают в себя не только банальные шагомеры, но и целую лабораторию в кармане, которая следит за тем, насколько активны вы были в течение дня и как в это время изменялось ваше сердцебиение, пульс и дыхание. Устройство анализирует информацию, дает рекомендации о том, сколько калорий вам нужно потреблять при таком образе жизни, а при малейшем подозрении на сбой в организме связывается в лечащим врачом. Все было бы хорошо, если бы информация о состоянии вашего здоровья интересовала только врача. В Великобритании уже распространена система, когда информация с фитнес-браслета попадет на рабочий стол работодателю, а тот передает ее в страховую компанию. В том случае, если человек активно занимался спортом, он может получить солидную скидку на медицинскую страховку. Остается только догадываться, что будет, если таким же образом страховые компании получат информацию о том, что у человека есть проблемы со здоровьем.

Дом милый дом

Системы умного дома, которые объединяют сразу несколько бытовых приборов и имеют выход в интернет, представляют особый интерес для хакеров всех мастей. Дух захватывает от того, какие перспективы для «творчества» предоставляет один только холодильник, который хозяева наделили полномочиями оценивать наличие продуктов и заказывать недостающие в интернет-магазине. Правда, пока о таких киберпреступлениях слышно не было. Намного более реальной выглядит угроза, связанная с голосовым управлением техникой. Дело в том, что помимо непосредственно команды умная техника в вашем доме запоминает и передает через интернет все громкие звуки, которые она различает в вашем доме. А что вы думаете об умном матрасе, в который встроены 24 датчика, способных фиксировать подозрительную активность и посылать уведомления об этом на смартфон хозяина? Так что будьте осторожны: следить за вами может даже собственный матрас.

ватной системой наблюдения, которую только предстоит разработать.

ИГЛА ВНУТРИ ЯЙЦА Чтобы вредоносная программа начала свое разрушительное действие, она должна сначала каким-то образом в компьютер попасть. Основной путь, по мнению экспертов, связан с производством компьютерного «железа», а именно — процессоров, куда внедряются те самые шпионские закладки.

— Возможность заложить такую закладку есть в любой микросхеме,— говорит Дмитрий Кузнецов.— Как сегодня происходит проектирование процессора? Есть кристалл, который делится на маленькие кусочки, и проектирование каждого из них отдается определенной команде. У того же Intel небольшой кусочек процессора проектируют лаборатории, входящие в состав Агентства национальной безопасности США. Что именно закладывается в эту часть кристалла, не знает никто. Раньше, когда кристаллы и элементы были очень большими, существовали довольно эффективные технологии их исследования: сотрудники отечественных спецслужб из соответствующих отделов слой за слоем срезали кристалл и анализировали эти элементы. Сейчас эти элементы настолько миниатюрные, что такой анализ провести просто невозможно. Поэтому теперь априори считается, что закладки там уже есть, но когда и для каких целей они сработают — неизвестно. Такой подход существует как в нашей стране, так, предположим, и в США, которые боятся подобных закладок в микросхемах, которые производятся в Китае.

Именно поэтому современные компьютерные системы проектируют так, чтобы сразу перекрыть возможность работы скрытых каналов. Например, вычислительную технику прячут в экранированные серверные, разделяют систему вентиляции так, чтобы не было передачи напрямую от компьютера во внешний мир, и так далее. Помимо этого, спецы по компьютерной безопасности тщательно следят за тем, чтобы компьютеры вдруг не начали вести себя странно, например включаться ночью или одновременно посылать подозрительное количество файлов. Для обнаружения более тонких процессов специалисты пишут специальные программы на основе вероятностных вычислений, которые отлавливают необычные случайные процессы. Другой, более традиционный способ борьбы со скрытыми каналами — зашумление киберпространства. Например, чтобы пресечь передачу данных через вентилятор, нужно сделать программу, которая будет специально менять скорость вращения вентилятора, и в итоге этот шпионский сигнал потеряется на фоне шума.

При этом, отмечают эксперты, утечка информации через скрытые каналы вряд ли когда-нибудь коснется рядовых граждан.

НЕВИДИМОЕ ОГРАБЛЕНИЕ Вообще, предотвращение всевозможных способов проникновения в компьютерные системы — головная боль для руководства всех стран. Считается, что эра киберпреступлений началась в 1983 году, когда студент Кевин Митник проник в глобальную сеть ARPANet — предшественник Internet, сумел войти в компьютеры Пентагона и получить доступ ко всем файлам Министерства обороны США. А несколькими годами позже 16-летний хакер Джонатан Джеймс взломал сервер НАСА и украл исходный код международной орбитальной станции МКС. С тех пор количество киберпреступлений растет как снежный ком.

— Чаще всего в своей повседневной жизни мы сталкиваемся с вирусами, червями и троянами, которые заражают компьютер или другие гаджеты благодаря нашей собственной беспечности,— говорит Дмитрий Кузнецов.— Как правило, пользователи устанавливают их сами под видом самых нелепых программ. Цель работы этих программ — собрать нужную информацию, например пароли от скайпа, почты или соцсетей, а затем передать их злоумышленнику. Единственное, что может остановить этот процесс,— антивирус, который обратит внимание, что гаджет использует непривычные для него порты. Поэтому задача вируса замаскировать свой сигнал так, чтобы он выглядел как обычный запрос в интернет.

Именно подобной маскировкой занято большинство хакеров средней руки. Чаще всего они незаметно крадут информацию, спрятав ее в большом массиве данных, который не вызывает подозрения. Например, сегодня можно записать текстовую информацию внутри видео- или аудиофайла так, что это почти не повлияет на вес файла. То есть вы вроде бы пересылаете видеоролик с семейного торжества своему коллеге из другого офиса, а на самом деле — это шифровка с коммерческой тайной. Подобных способов спрятать информацию очень много, поэтому пока отследить их практически невозможно.

В первую очередь современных киберпреступников интересуют платежные системы. На прошлой неделе Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT) опубликовал данные, согласно которым с июня 2015 года по май 2016 года было зафиксировано более 20 крупных кибератак на платежные системы кредитных организаций. В итоге в общей сложности хакеры украли около 1,37 млрд рублей у российских банков. При этом эксперты утверждают, что если еще в прошлом году хакеров больше интересовали личные счета граждан, то теперь они переключились на сами банки и платежные системы с их нововведениями по картам, интернет- и мобильному банку.

Правда, в последние 2–3 года не менее широким полем для деятельности хакеров стал «интернет вещей», то есть все гаджеты, которые работают дома и имеют выход в Сеть. Хакеры атакуют кредитные карты и автомобили, взламывают электронные редакции газет и серверы, хранящие медицинскую информацию пациентов. «Хитами» нынешнего года стал взлом радионяни и электронного унитаза. Родители трехлетнего малыша в Сан-Франциско выяснили, что хакер пугал ребенка по ночам, разговаривая с ним через устройство. Программируемый унитаз вывела из строя группа хакеров, получив доступ ко всем функциям гаджета. Так, они могли в любой момент включить спуск воды и испугать посетителя туалета. Эксперты считают, что скоро мы будем тратить на защиту своих гаджетов столько же средств, сколько и на их покупку. Насколько реальны подобные прогнозы, нам предстоит выяснить в ближайшее время. ■■