Незримый бой

А. ГОЛЫШКО, канд. техн. наук, г. Москва

"Секрет успеха — искренность. Если вы можете её изобразить, дело сделано".

Граучо Маркс (американский комик)

Верю — не верю

Вроде бы недавно говорили про информационную безопасность (ИБ), и вот опять. Впрочем, ничего удивительного нет — есть лишь удивительное и порой незаметное развитие всё новых и новых новостей из мира ИБ, обеспечивать и нарушать которую стараются много и регулярно.

Бурный рост объёма персональных больших данных имеет далеко идущие последствия. Вне всякого сомнения, цифровой образ каждого индивидуума будет играть немалую роль в определении его места в мире. Более того, вся эта информация уже сама по себе имеет огромную ценность для интернет-гигантов, для розничной торговли, для компаний, оказывающих финансовые услуги, и многих других. Даже в самый обычный день мы оставляем за собой широкий информационный след. История посещения интернет-сайтов, онлайновые предпочтения, покупательские привычки, принимаемые на работе решения, социальное взаимодействие — всё это переводится в двоичный код, вызывая сложное взаимодействие запросов и ответов, подтверждений и отказов. Когда же в полную мощь заработает Всеобъемлющий Интернет (IoE) и сегодняшние 10 миллиардов подключённых объектов превратятся к 2020 г. в 50 миллиардов, вполне вероятно, наша одежда, наши дома, автомобили, шкафы и холодильники будут передавать всё больше и больше информации о себе и нас самих. Всё бы хорошо, если бы не одно "но"...

Не хотелось пугать, но вот, к примеру, согласно совместному исследованию "Лаборатории Касперского" и агентства B2B International, в России доля компаний, столкнувшихся с внешними киберугрозами за последние 12 месяцев, выросла и вплотную приблизилась к 100 %. И самой значимой внешней угрозой по-прежнему являются вредоносные программы — именно они стали причиной инцидентов у 77 % респондентов.

Вторая по опасности внешняя угроза для компаний — спам. С неприятными последствиями получения нежелательной корреспонденции столкнулись 74 % респондентов. Это неудивительно, так как зачастую спам содержит вложения — те же вредоносные программы, запуск которых на незащищённой машине влечёт за собой утечку информации. Существенно выросла доля корпоративного шпионажа — до 32 %, в основном за счёт сильного увеличения доли подобных инцидентов в больших организациях.

Зато, как показало другое исследование тех же компаний, 13 % опрошенных интернет-пользователей в России не верят в реальность кибератак. По их мнению, угроза преувеличивается компаниями, разрабатывающими инструменты информационной безопасности. Причём даже те, кто знает об угрозах, отнюдь не всегда от них защищаются, только 15 % думают, что могут стать целью киберпреступников, и лишь 22 % респондентов в России не опасаются взлома своих онлайн-аккаунтов. Ну а абсолютное большинство полагают, что их данные не могут быть интересны злоумышленникам. Тем временем практически любой компьютер, смартфон или планшет может быть использован преступниками, например, в качестве бота для рассылки спама, организации DDoS-атак или отправки фишинговых ссылок через мессенджеры и электронную почту. В частности, в 2014 г. 36 % финансовых компаний в России столкнулись с утечкой данных по денежным операциям. При этом 81 % финансовых организаций считает, что они "принимают все необходимые меры для поддержания актуальности защитных технологий".

Инновационный тормоз

Недавно компания Intel призвала ведущие компании в области ИКТ-технологий, здравоохранения и медицины обратить особое внимание на вопросы конфиденциальности данных. Малкольм Харкинс, вице-президент и директор по безопасности и конфиденциальной информации этой компании, заявил, что возможность новых открытий находится под угрозой и призвал представителей отрасли быть более открытыми и ответственными при сборе и использовании данных пользователей. С одной стороны, перед нами открываются небывалые возможности для внедрения инноваций, что, в определённой степени, связано с расширением наших возможностей для вычислений, хранения и анализа "больших данных", но эти возможности также создают неопределённости и опасения среди людей. С другой стороны, темпы развития инноваций будут тормозиться недоверием людей в отношении того, что компании знают о них и как они используют их личную информацию.

Недавний опрос, проведенный компанией Harris Poll, демонстрирует недостаток понимания и доверия в отношении того, как используются персональные данные пользователей. Большинство респондентов (84 %) считают, что определённые данные о них или с их устройств продаются третьим сторонам. Практически две трети владельцев устройств признают, что они не знают, кто получает доступ к данным на их устройствах и как они используются. Более того, половина жителей США не способна правильно определить значение термина "анонимизированные данные", что подтверждает тот факт, что пользователи не знают о том, как их личная информация может быть защищена. При обсуждении конкретных преимуществ распространения их данных участники опроса продемонстрировали готовность обмена информацией, если их персональная информация будет обезличена.

К Intel присоединились Siemens, Personal, Sensity, Privacy Analytics, Knewton, TrustLayers др., которые получают всё больше социальных ценностей от анализа "больших данных" (Big Data), что требует обеспечения надёжной защиты данных пользователей от неправильного использования.

Фальшивые сети

Поставщик технологий защиты информации, компания ESD America, в ходе совместного эксперимента со своими клиентами обнаружила в США более 20 подозрительных базовых станций сотовой связи, которые не имели стандартных идентификаторов и были установлены на военных объектах. В компании заявили, что эти станции предназначены для перехвата сигналов с мобильных телефонов и дистанционного внедрения "жучков". ESD America предлагает своим клиентам защищённый смартфон GSMK CryptoPhone 500 ценою в 3,5 тыс. долл. США, с помощью которого и были отслежены станции-перехватчики и который представляет собой модификацию Samsung Galaxy S3 с кастомизированной (от англ. custom — потребитель — адаптация товара или услуги под конкретного покупателя с учётом его требований и пожеланий) версией Android, которая не только предоставляет дополнительный уровень защиты данных, но и позволяет отражать внешние атаки на устройство.

Перед тем как включить "прослушку", эти станции отправляли на мобильное устройство команду для отключения 4G и перехода на 2G. Поскольку 4G является более защищённым, 2G взломать проще. А чтобы внезапный переход с 4G на 2G на вашем телефоне не бросился вам в глаза, современные перехватчики умеют маскироваться и заставляют устройство отображать 4G, хотя в действительности аппарат уже переключился на тот стандарт, который проще взломать. На вопрос о том, кто же расставил эти базовые станции, эксперты ESD America лишь намекнули на их среднюю цену около 100 тыс. долл. США и на правительство, которому "по плечу" такие траты. Кстати, в марте 2014 г. гендиректор ESD America признался изданию Technology Review, что после раскрытия сведений о масштабах деятельности АНБ Эдвардом Сноуденом спрос на CryptoPhone 500 вырос в три раза, и к моменту интервью в мире уже было около 100 тыс. пользователей

этих аппаратов, поскольку разговоры шифруются только между их владельцами.

Шифрованием персональной информации занялись и крупнейшие компании, поэтому в конце сентября 2014 г. директор ФБР Джеймс Коми заявил, что его серьёзно беспокоят предпринятые Apple и Google усилия по шифрованию данных пользователей iOS и Android. К примеру, в новой версии Android даже правительственные организации не смогут получить доступ к хранящимся на устройствах файлам, аналогичная защита реализована и в iOS 8, выпущенной в середине сентября. Глава спецслужбы считает, что правительственные организации всё же должны иметь доступ к данным граждан в экстренных случаях, например, когда речь идёт о террористической атаке. Коми также отметил, что спецслужбы могут изучать содержимое чужого шкафа или смартфона только при наличии судебного ордера, однако факт существования шкафа, который нельзя открыть ни при каких обстоятельствах, кажется ему бессмысленным, ведь речь, к примеру, может идти о похищении детей. Глава ФБР уверен, что наверняка настанет день, когда для спасения жизни людей необходимо будет получить доступ к устройству с зашифрованной информацией и ему не хочется впоследствии отвечать на вопросы о том, почему эти жизни не удалось спасти.

Дыра в доверии

Как сообщили в октябре специалисты по информационной безопасности из компании FireEye, в операционной системе iOS обнаружена серьёзная уязвимость, с помощью которой хакеры могут распространять вредоносные приложения, подменяющие на мобильном устройстве подлинные программы, такие как приложения для работы с электронной почтой и доступа к банковским счетам. Это означает, например, что хакер может узнать персональные банковские данные пользователя, заменив подлинное банковское приложение на фальшивое с похожим интерфейсом. Пользователь при этом может ничего не заметить, так как фальшивка будет имитировать функциональность оригинала. Надо сказать, что эта новость серьёзно встревожила деловые круги по обе стороны океана.

В свою очередь, разработчики Replicant, свободного дистрибутива Android, обнаружили бэкдор (лазейку) в устройствах на базе Android, выпускаемых компанией Samsung Electronics, позволяющий третьим лицам получать удалённый доступ к файловой системе мобильного устройства. Современные мобильные устройства оснащаются двумя отдельными процессорами: процессором приложений, которым управляет операционная система, в данном случае Android, и сигнальным процессором, который отвечает за связь с мобильной сетью. Бэкдор присутствует именно в ПО сигнального процессора. Сигнальные процессоры управляются проприетарными операционными системами (т. е. разработанными самими производителями чипов), и содержащиеся в них лазейки позволяют превратить процессор в "жучок". "Нехороший человек" может включить микрофон, снять GPS-данные и получить доступ к камере, а также к сохранённым в памяти устройства пользовательским данным. Ну а поскольку мобильные устройства постоянно подключены к сети через сигнальный процессор, шпионить можно непрерывно. К тому же в большинстве современных устройств сигнальный процессор тесно связан с процессором приложений и с прочими компонентами, поэтому изолировать его невозможно.

В ноябре Федеральная торговая комиссия (ФТК) США запросила у Apple гарантии того, что смарт-часы Apple Watch, о которых уже рассказывалось на страницах журнала, а также другие мобильные устройства, собирающие информацию о здоровье пользователя, не будут передавать эти данные третьим лицам. Представители ФТК провели несколько встреч с сотрудниками Apple, на которых представители компании заверили чиновников, что данные о здоровье пользователей никак не могут попасть к третьим лицам и не будут передаваться сторонним разработчикам приложений для устройств Apple. Сообщается, что Apple сотрудничает с регуляторами стран, где продаётся её продукция, для обеспечения её соответствия местному законодательству и объясняет встроенные в продукты механизмы защиты данных. При этом основная часть данных, которые собирает Apple Watch и приложение HealthKit, не подпадает под действие американского закона HIPAA (Health Insurance Portability and Accountability Act — федеральный закон, в котором установлены правила обмена личной медицинской информацией и её защиты от неразрешённого использования). Тем не менее ФТК настаивает на том, что данная информация всё ещё является крайне личной и следит за тем, как её собирают, защищают и распространяют.

Ещё в сентябре вопросами сохранности данных о здоровье пользователей устройств Apple заинтересовался главный прокурор штата Коннектикут Джордж Джепсен, который обратился к руководству компании с соответствующим письмом.

Четыре пути России

Темой заседания Совета Безопасности РФ, состоявшегося 1 октября 2014 г., были вопросы противодействия угрозам национальной безопасности в информационной сфере, актуальность которой резко возросла в условиях обострения отношений России с рядом западных стран. В своём выступлении на СБ глава государства, в частности, отметил возрастающую роль информационных технологий для общества, экономики и обеспечения жизнедеятельности государства в целом и заявил, что государство не намерено ограничивать доступ в Интернет, ставить его под тотальный контроль, огосударствливать, а также ограничивать законные интересы и возможности людей, общественных организаций, бизнеса в информационной сфере. *"Надёжная работа информационных ресурсов, систем управления и связи, имеет исключительное значение для обороноспособности страны, для устойчивого развития экономики и социальной сферы, для защиты суверенитета России в самом широком смысле этого слова,* — подчеркнул президент, — *необходимо учитывать и существующие в информационной сфере риски и угрозы. Мы видим, что отдельные страны пытаются использовать своё доминирующее положение в глобальном информационном пространстве для достижения не только экономических, но и военно-политических целей. Активно применяют информационные системы в качестве инструмента так называемой мягкой силы для достижения своих интересов"*.

При этом на заседании было подчёркнуто, что сегодня России необходимо сформулировать и реализовать комплекс дополнительных мер в области ИБ, и сформулировано четыре основных направления работы в этом направлении:

— качественно повысить защищённость отечественных сетей связи и информационных ресурсов, в первую очередь тех, что используют государственные структуры, стремиться исключить незаконное вмешательство в их работу, а также утечку конфиденциальной и персональной информации;

— обеспечить устойчивость и безопасность российского сегмента Интернета, но при этом защитить граждан от сетевых рисков и угроз, используя при этом практику, которая уже применяется во многих странах мира;

— развивать отечественные технологии, технику и информационные продукты, эффективно стимулируя при этом их использование госструктурами и нашими компаниями;

— расширять сотрудничество в сфере обеспечения международной ИБ с глобальными и региональными организациями.

Принимавший участие в работе СБ глава Минкомсвязи Николай Никифоров позже пояснил журналистам, что в значительной мере обсуждение проблемы обеспечения ИБ шло на основании анализа результатов, полученных в ходе июльских учений по защите российского сегмента Интернета, которые проводились совместно с ФСБ и Минобороны на площадке Минкомсвязи. В ходе этих учений имитировалось отключение извне (со стороны правительства США и американского регулятора Интернета ICANN) российских доменных зон. Министр также сообщил, что Россия намерена формировать дублирующие элементы сетевой инфраструктуры для повышения безопасности российского сегмента, подчеркнув при этом, что эта работа будет вестись в сотрудничестве с членами БРИКС и ШОС. Независимые эксперты уверены, что главным партнёром в этой деятельности может быть Китай, который работает в направлении создания

альтернативной интернет-инфраструктуры уже много лет.

Вместе с тем министр отметил, что угрозы, возникающие в результате использования зарубежных компьютерных и мобильных устройств, являются сильно преувеличенными. В частности, безопасность служебной информации должна обеспечиваться за счёт применения защищённых каналов связи, о чём недавно ещё раз было доведено до сведения чиновников различного уровня. Правда, всех остальных это, похоже, не касается.

Когда очень хочется

В конце октября правительство Великобритании впервые подтвердило информацию о том, что национальные спецслужбы имеют доступ к данным британцев без соответствующего разрешения суда. Этот факт был признан уполномоченной комиссией по надзору за скрытой слежкой после того, как представители правозащитных организаций Privacy International и Liberty and Amnesty International направили иск в специальный Трибунал по расследованию превышения спецслужбами своих полномочий. В докладе комиссии отмечается, что британские спецслужбы имеют несанкционированный доступ к широкому кругу данных граждан, а также к данным, которые предоставляют им разведывательные службы из других стран, включая АНБ США. При этом доступ осуществляется без разрешения суда.

Уже в ноябре немецкая разведка объявила, что планирует создать систему раннего предупреждения о готовящихся на государство кибератаках. Для этого она планирует шпионить за пользователями социальных сетей за пределами Германии (несмотря на протокол шифрования HTTPS), и на это планируется потратить 300 млн евро. Данная программа называется Strategic Technology Initiative (STI). По данным издания Spiegel, часть своего бюджета служба планирует потратить на ещё одну программу под названием Nitidezza. Её суть заключается в покупке на чёрном рынке неизвестных или неопубликованных уязвимостей, которые бы смогли облегчить работу немецких агентов. До 2020 г. на эти цели зарезервировано 4,5 млн евро. Уж не работали ли немецкие агенты над iOS?

Ядерное ПО

Как следует из текста на сайте Еврокомиссии, европейские власти планируют приравнять легальное шпионское программное обеспечение, разрабатываемое местными компаниями для государственных заказчиков, к технологиям двойного назначения и поставить его в один список с ядерными реакторами, камерами со сверхвысоким разрешением и ракетным топливом. То есть теми продуктами и технологиями, которые "обычно служат гражданским целям, но могут быть использованы в военной сфере и для распространения оружия массового поражения". Поправки в список продуктов и технологий двойного назначения были переданы Европарламенту и Евросовету. В случае их согласия, обновлённый список, содержащий шпионское ПО, должен вступить в силу в конце декабря 2014 г.

Примером шпионского ПО, о котором идёт речь, является FinFisher — решение, продажей которого занимается британская компания Gamma International. Согласно описанию на официальном сайте, Finfisher позволяет "выполнять удалённое наблюдение и инфицирование" и способен предоставить "полный доступ к хранимым данным с возможностью получения контроля над целью". FinFisher позволяет взламывать компьютеры под управлением операционных систем Windows, OS X и Linux, а также мобильные устройства на базе Android, iOS, Windows Phone, BlackBerry и Symbian. Решение позволяет получать доступ к аккаунтам сервисов электронной почты, таких как Gmail, Outlook и Yahoo, а также взламывать учётные записи Skype-сервиса, считающегося одним из самых надёжных на рынке благодаря применяемым в нём технологиям шифрования данных.

Согласно документам, оказавшимся в распоряжении The Guardian, в 2010 г. Gamma International предложила за 287 тыс. долл. США купить FinFisher правящему в Египте режиму для подавления оппозиции. В сентябре 2014 г. сайт Wikileaks опубликовал сведения о том, что FinFisher используется правительственными организациями в Австралии, Бахрейне, Бангладеше, Бельгии, Боснии и Герцеговине, Эстонии, Венгрии, Италии, Монголии, Нидерландах, Нигерии, Пакистане, Сингапуре, Словакии, Южной Африке и Вьетнаме.

В октябре был выпущен отчёт OpenNet Initiative, в котором говорилось, что аналогичное шпионское ПО, разработанное компаниями в США и Канаде, используется в девяти странах на Ближнем Востоке и в Северной Африке для ограничения доступа к сайтам с политическими, социальными и религиозными материалами.

Тот факт, что правительства самых разных стран, которым искренне доверяют их граждане, разрабатывают и используют подобное ПО, уже не секрет. На эту тему, к примеру, в августе 2014 г. на конференции BlackHat выступил директор по исследованиям компании F-Secure Микко Хиппонен: "Не так давно идея о том, что западные демократические государства замешаны в разработке вредоносных программ, казалась дикостью. А как вам такая идея — западные демократические государства оставляют лазейки в системах связи, чтобы следить за другими демократическими государствами? Это именно то, что происходит сейчас".

Смена приоритетов

Можно долго дискутировать о сохранности персональных данных, и, скорее всего, каждое государство сделает в этой сфере так, как посчитает нужным, что бы ни утверждала общественность и правозащитники. Что же касается всего остального, то там возможно всякое. Например, можно снять ответственность за хранение целого ряда персональных данных пользователей, которые выложили о себе всё что можно (и даже что нельзя в приличном обществе) в социальных сетях. Ну разве что банковские данные требуют сохранности, чем, впрочем, банки и занимаются. Но зачем наказывать каких-то провайдеров за нарушения правил хранения того, что, по-видимому, не представляет никакой ценности для их владельцев по сравнению с их желанием громко заявить о себе?

Или что будет, если потребители будут охотно делиться персональными данными за вознаграждение? В таком случае вопросы приватности уйдут на второй план, потому что помимо приобретения сомнительной известности можно ещё и заработать. При этом могут пострадать и такие веб-гиганты, как Google. К примеру, сегодня большинство их пользователей бесплатно предоставляют свои данные. Но что если какой-нибудь конкурирующий поисковик совершенно искренне предложит хотя бы 10 центов за поисковый запрос? Рынок поисковых машин может в одночасье кардинально перемениться, а целый слой хакеров, как в известном фильме, будет вынужден с горечью признать, что "всё украдено до нас".

*По материалам **"Лаборатории Касперского", Cisco, Intel, PCWeek, CNews, The Guardian, РИА Новости, The Huffington Post, Popular Science, Reuters**.*