# Борьба за жизнь в информационном обществе

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

*"Об этом человеке известно только, что он не сидел в тюрьме, но почему не сидел — неизвестно".*

**Марк Твен**

## Динамика угроз

Обустраиваясь в глобальном информационном обществе, нетрудно заметить, что все проблемы и угрозы тоже становятся глобальными. И бороться с ними следует также в глобальном масштабе. Но сначала надо понять масштаб проблемы.

Как сказано в докладе американского оператора **Verizon**, киберпреступники используют для взлома сетей те же уловки, что и восемь лет назад. Причиной тому большое число слабо защищённых участков сетей, представляющих для них лёгкую добычу. Однако, несмотря на значительный рост числа случаев утечки данных, было отмечено значительное сокращение случаев краж информации. Вероятно, это следствие того, что мощная защита крупномасштабных процессов обработки данных сети вынуждает искать несильно защищённые цели, даже если потенциальный доход от них невелик, так как при взломе таких сетей риск быть пойманным минимален.

Согласно исследовательским организациям по утечкам информации в 2010 г., зафиксировано 1014 случаев, что на 15,6 % больше показателя 2009 г. В России зафиксировано 37 инцидентов, что на 60,9 % больше, чем в 2009 г. Основными источниками утечек (суммарно 76 %) стали государственные организации, медицинские и образовательные учреждения, финансовые и торговые компании. При этом число обнародованных утечек составляет в лучшем случае 0,1 % от их фактического количества. Это связано с отсутствием законодательно закреплённых требований обнародовать инциденты и с несовершенством применяемых мер защиты. В 2010 г. произошёл значительный рост доли утечек через мобильные накопители (4,4 %) и web-сервисы (3,2 %). В основном утекают персональные данные (63,6 %) клиентов и сотрудников. Однако несмотря на рост общего числа случаев в 2010 г., значительно уменьшился общий ущерб от всех утечек, а также средний показатель ущерба от каждого из инцидентов. Кроме того, заметно сократилось и число утерянных записей. Этот факт можно объяснить массовым внедрением систем предотвращения утечек конфиденциальных данных (Data Loss Prevention — DLP) и общей активизацией мер, направленных на борьбу с утечками, особенно в США, где всё чаще компании сталкиваются со штрафами и прочими негативными последствиями допущенных утечек.

Географические данные на сегодняшний день наглядно показывают, насколько подходы к проблеме защиты от утечек конфиденциальной информации разнятся в зависимости от страны и действующих там законов. Так, большая часть из обнародованных утечек по-прежнему относится к США, в то время как в России ставшие достоянием гласности инциденты можно пересчитать по пальцам, однако даже они смогли затронуть интересы огромной части населения. Кроме того, несмотря на формальную принадлежность **Google**, **Facebook**, **Gawker Media** и других крупных организаций к США, связанные с ними утечки коснулись интересов людей во всём мире, в том числе и российских пользователей. Перекос данных в сторону США объясняется действующим там законодательством, согласно которому организация обязана сразу же уведомить всех пострадавших, а в ряде случаев и компенсировать их реальные и потенциальные убытки.

Как свидетельствует отчёт **Cisco Security Intelligence Operations (SIO)**, киберпреступники перешли от массовой рассылки спама к целенаправленным атакам, способным принести куда больший куш. В целом объёмы спама падают. За период с июня 2010 г. по июнь 2011 г. число ежедневно передаваемых спам-сообщений сократилось с 300 млрд до 40 млрд. Наряду с этим, за тот же период произошёл трёхкратный рост целенаправленных фишинг-атак (spearphishing) и четырёхкратный рост мошеннических атак против конкретных лиц, а также заражений вредоносными программными кодами. Атаки киберпреступников наносят большой ущерб: корпорации ежегодно терпят от них убытки в размере 1,29 млрд долл. США. При этом атаки начинаются с малозаметных действий злоумышленников против конкретного человека или группы сотрудников. Для этого обычно используют вредоносные программные коды или устойчивые вредоносные системы долгосрочного действия, рассчитанные на то, чтобы в течение определённого времени постепенно добыть нужные киберпреступникам данные.

Даже в тех случаях, когда киберпреступники организуют целенаправленную атаку на десяток руководителей крупных компаний (в отличие от грубой массовой рассылки спама), они обычно сосредоточивают усилия на ком-то одном в надежде получить максимальную прибыль. Средняя окупаемость целенаправленной атаки может в 40 раз превысить окупаемость массовых рассылок, если жертва имеет доступ к корпоративным банковским счетам. В дополнение по данным **Cisco SIO**, в среднем репутационный ущерб составляет 1900 долл. на каждую взломанную пользовательскую систему, в 6,4 раза превышая прямые финансовые потери.

Американский Департамент внутренней безопасности провёл исследование систем ИТ безопасности, чтобы выяснить наиболее типичные изъяны, которыми потом пользуются хакеры для кражи данных. В результате исследования была в очередной раз подтверждена известная истина — человек является самым слабым звеном ИТ безопасности. Персонал американских государственных учреждений в обход принятых норм безопасности приносил с собой из дома флеш-носители, внешние жёсткие диски и даже ноутбуки, сохраняя там рабочую информацию или создавая условия, которыми в будущем могут воспользоваться хакеры. Тест показал, что нынешние автоматизированные средства безопасности сравнительно неплохо защищают компьютеры, однако злоумышленники всё чаще для вторжения используют банальную человеческую глупость. К примеру, очень часто хакеры подделывают сообщения от известных компаний, таких как **Google**, **Intel**, **Facebook** или **Twitter**. При этом ИТ злоумышленники постепенно уходят от массовых кампаний, предпочитая индивидуальные рассылки и целевые атаки. Именно в одной из таких целевых атак была поражена компания **RSA Security**, которая "поделилась" с хакерами данными о ключах идентификации SecureID. В результате дополнительные затраты на повторный выпуск и дистрибуцию составят от 50 до 100 млн долл.

Вторым по популярности излюбленным способом атак является целевое распространение вредоносных файлов со встроенными эксплоитами (т. е. программами, использующими ошибку в ПО для выполнения некоторых действий в атакуемой системе). Здесь лидерами являются продукты **Adobe Systems** — Flash и Reader. В отчёте говорится, что одним из значительных трендов стали атаки на руководителей высшего звена, которые по роду своей

деятельности обладают доступом к информации, что является наиболее притягательным для хакеров моментом. С другой стороны, топ-менеджеры — это те же люди. При этом, как констатируют специалисты, ещё не созданы технологии или устройства, которые спасут людей от их же собственной глупости.

О том же самом свидетельствуют угрозы безопасности мобильного банкинга, которые по обыкновению заключаются не в ИТ инфраструктуре самого банка и не в каналах передачи данных мобильных операторов, а в самом клиенте и его мобильном терминале. Причём банк не может контролировать клиента и указывать ему правила безопасного поведения при работе со счётом — он может лишь обратить на это его внимание. Согласно недавнему исследованию **Ponemon Institute** в США, 29 % владельцев телефонов хранят в них данные о своих пластиковых картах, 90 % понятия не имеют, что сами могут загрузить на телефон шпионскую программу и опять же 90 % людей не знают, что финансовые приложения для смартфонов передают в Интернет детали платежа, включая данные о карте. Следует также заметить, что случаи реальных мошеннических действий со счетами клиентов через мобильные устройства банки предпочитают не разглашать, опасаясь за свою репутацию.

В сентябре антивирусные аналитики **Symantec** заявили об обнаружении новых методов социальной инженерии, ориентированной на введение пользователей в заблуждение или их открытый шантаж с целью кражи денег с банковских счетов или их персональных данных. Отмечается и более активное использование сравнительно новых технологий, таких как HTML 5, для создания поддельных сайтов и мобильного ПО. Мошенники начали активнее применять JavaScript для разработки вредоносного ПО и различных мошеннических трюков.

Летом в США был уволен руководитель Службы быстрого реагирования на компьютерные угрозы Министерства внутренней безопасности США Рэнди Викерс. Отставке предшествовал ряд громких хакерских атак на правительственные сайты. В частности, в июле 2011 г. стало известно, что хакеры из группировки Anonymous взломали сервер компании **Booz Allen Hamilton**, которая является подрядчиком Пентагона. В результате этой атаки киберзлоумышленники похитили электронные адреса 90 тыс. американских военных. Кроме того, другая известная группировка — Lulz Security, дружественная группировке Anonymous, — в этом году провела несколько чрезвычайно резонансных акций, в том числе взлом сайта ЦРУ, сайта одного из подразделений ФБР, а заодно и внутреннюю сеть Сената США.

## Вся жизнь — борьба

Киберпреступность, как правило, — составная часть обычной преступности. Иногда криминал может обойтись и без неё. В частности, в отдельных местах нашей планеты мобильный банкинг более безопасен, чем традиционное посещение отделения банка, потому что у клиента гораздо больше шансов быть ограбленным по пути к отделению банка, чем путём кражи персональных данных. Поэтому борются со всем этим все, везде и по разным направлениям. И бороться впредь предстоит широким фронтом, т. е. комплексно, и заранее очевидно, что это обойдётся недёшево.

Услуги информационной безопасности (ИБ) — одни из самых востребованных. По данным **IDC**, объём российского рынка ИБ в 2010 г. составил 119 млн долл. Сюда входят услуги анализа интернет-трафика и web-фильтрации, защиты от DDoS-атак (Distributed-Denial of Service — распределённая атака типа "отказ в обслуживании"), спама и вирусов, контентной фильтрации трафика, управления межсетевыми экранами, системами аутентификации и авторизации, системами обнаружения и предотвращения вторжений, криптографическими системами и пр.

В частности, как советуют китайские специалисты, для качественной защиты необходимо организовать систему контроля, охватывающую ключевые национальные сетевые узлы. Во-вторых, обеспечить, чтобы система контроля вовремя обнаруживала, идентифицировала, отслеживала и перехватывала вредоносные действия в сети и контент определённых преступников. В-третьих, система контроля интегрирует, коррелирует, разумно оценивает и хранит массовую интернет-информацию, выясняет полезную информацию о потенциальных преступниках или террористах, предсказывает и исправляет критические ситуации и предоставляет доказательство осуществления киберпреступления для соответствующих органов власти.

Компанией **Huawei** разработана система, которая предоставляет мониторинг, сбор данных и отслеживание активности в сети на основе объекта или IP-адреса в режиме реального времени и выполняет функции интеллектуальной платформы для анализа больших объёмов данных. Платформа обеспечивает функции уведомлений перед событием, последующего анализа и запросов для всех основных событий. Отслеживается поведение в сети всех пользователей в своём домене, определяются различные форматы файлов в сети — текстовые, изображения, видео, аудио, а также SMS во всех сетях, включая локальные, фиксированные и мобильные всех стандартов. Подобная система помогает правовым органам легально осуществлять мониторинг общественных мнений online, выявлять и блокировать нелегальные или террористические действия, управлять обычным поведением в сети и ограничивать распространение вредоносных контентов.

Компания **Cisco** предпринимает превентивные действия по борьбе с целенаправленными атаками, используя для этого информацию об угрозах, поступающую в реальном времени из **Cisco SIO**. Эта самая крупная в мире "облачная" экосистема информационной безопасности использует базу данных, куда поступает информация от миллиона работающих решений **Cisco** для электронной почты, web-сервисов, межсетевых экранов и систем предотвращения вторжений. Собранные данные **Cisco SIO** анализирует и обрабатывает, автоматически классифицируя угрозы и создавая правила на основании более двухсот параметров. Кроме того, специалисты по информационной безопасности принимают и передают информацию об угрозах, способных принести наибольший ущерб сетям, приложениям и устройствам. Правила предотвращения угроз передаются на устройства безопасности **Cisco** в динамическом режиме в течение 3…5 мин. При этом в компании говорят, что ни одна система не способна работать со 100 %-ной надёжностью, но в условиях нарастающих целевых атак ИТ руководители и специалисты, приобретающие средства информационной безопасности, ни на секунду не должны забывать о полномасштабных решениях, работающих в реальном времени.

Компания **Google** анонсировала запуск новой онлайновой системы предупреждения о наличии злонамеренного ПО на сайтах, которые выдаются в результатах поиска. Новая система предупреждает пользователя, работающего с результатами поисковика о том, что, переходя на тот или иной ресурс, пользователи рискуют заразить компьютер вредоносным ПО.

Власти Сеула создают интегрированную систему глобального анализа интернет-трафика, а также собственную операционную систему на базе Linux для установки на сетевые шлюзы, которые позволят успешнее бороться с нарастающим в адрес Сеула потоком DDoS-атак. В правительстве Кореи говорят, что параллельно с этим намерены построить современную автоматизированную систему управления движением автотранспорта по всему городу, что позволит, с одной стороны, снизить количество пробок, а с другой — быстрее реагировать на чрезвычайные ситуации. Новая система анализа сетевого интернет-трафика позволит практически в реальном масштабе времени обнаруживать и блокировать DDoS-атаки и попытки взлома ИТ систем, обслуживающих критически важные городские инфраструктуры. Новая система будет в постоянном режиме сканировать все работающие компьютерные городские узлы и находить всю подозрительную активность.

В скором времени в Индии будут приняты нормы, регулирующие вопросы безопасности в области телекоммуникаций. Один из пунктов будет предусматривать, что 50 % базового сетевого оборудования должно быть произведено или разработано в Индии. Все производители и мобильные опе-

раторы должны будут стремиться к обеспечению этой нормы, как предусмотрено проектом Telecom Security Policy.

Иногда подобное "лечится" подобным. В частности, пока ещё не до конца созданная социальная сеть AnonPlus, о работе над которой заявила хакерская группа Anonymous, недавно сама стала жертвой хакеров ранее неизвестной группы Turkiye.

Недавно юристы **Microsoft** одержали окончательную победу над владельцами одного из самых крупных мировых спам-ресурсов; после того как они выиграли дело, компания получила контроль над более чем 20 серверами и IP-адресами сети Rustock. Право собственности над оборудованием перешло к компании **Microsoft** в декабре прошлого года, после того как федеральный судья штата Вашингтон вынес решение в пользу **Microsoft** по их иску против сети Rustock, поразившей 1,6 млн персональных компьютеров и отправлявшей по 30 миллиардов спам-сообщений в сутки. Согласно судебным документам, основатель Rustock — гражданин России, в сети известный под ником Cosma2k, приобрёл IP-адреса, на которых размещались многие командные и контрольные серверы. Следователи **Microsoft** предъявили ему обвинения в распространении вредоносных программ и причастности к спам-рекламе фармацевтических препаратов. В **Microsoft** полагают, что всего им предстоит отыскать в России 11 человек. Специалисты полагают, что решимость **Microsoft** в поисках Cosma2k и его соратников может принести дополнительную пользу, показывая потенциальным главам бот-сетей, что у их преступных деяний могут быть последствия, неважно в какой точке земного шара они находятся.

В августе американские голливудские студии, звукозаписывающие компании и независимые ассоциации артистов в сотрудничестве с американскими интернет-провайдерами **AT&T Inc., Comcast Corp.** и **Verizon** презентовали новое программное обеспечение для уведомления интернет-пользователей о том, что их аккаунты используются для доступа к фильмам, музыкальным записям и иному контенту без соответствующей авторизации, т. е. для онлайн-пиратства. Также новая система уведомляет пользователей, скачивающих данные по чужим реквизитам. Такие пользователи тоже могут получить уведомления от провайдера, причём в отношении этой группы пользователей поставщик интернет-услуг может применять различные меры: от полного отключения до замедления скорости доступа и блокировки ресурсов.

Кстати, в прошлом году Министерство обороны США создало новую военную структуру — Киберкомандование. Выяснилось, что существующая киберстратегия недостаточно эффективна и необходимо предусмотреть принятие более решительных мер с тем, чтобы потенциальные агрессоры поняли, что их ждёт суровое наказание за попытку взломать компьютерные сети правительства США.

В сентябре управление "К" МВД России сообщило о пресечении деятельности мошенников, зарабатывавших на отправке платных SMS-сообщений через телефоны абонентов всех мобильных операторов. Преступники использовали для этого специальное оборудование, позволявшее управлять мобильными телефонами (сообщалось, что оно не имеет аналогов в России).

Недавно в России создано некоммерческое партнерство **"Лига безопасного Интернета"**, куда вошли операторы **"МТС"**, **"ВымпелКом"**, **"МегаФон"**, **"Ростелеком"**, почтовый сервис Mail.ru и "Лаборатория Касперского". Уже разработан подробный план действий и, в частности, планируется создать центр мониторинга и кибердружины.

## Ваш "друг" смартфон

Британские правоохранительные органы успешно используют информацию, полученную из смартфонов. Где вы были, с кем разговаривали, с кем спали — секреты, которыми люди не делятся даже с ближайшими друзьями, свободно получает устройство, знающее вас лучше любого свидетеля. В прошлом году Национальное Агентство Соединённого Королевства по развитию полиции сделало получение "мобильных свидетельств" одним из своих главных обучающих курсов, а мобильные устройства теперь массово отправляются судебным экспертам для анализа того, где они побывали и что содержат (изображения, записи, логи звонков, основанная на базовых станциях и Wi-Fi-сетях информация о местонахождении, навигационная информация и пр.).

Как сообщают юристы, у полиции есть очень широкие права на проверку содержимого мобильных телефонов, если существует "обоснованное подозрение", что обладатель телефона совершил преступление. Погрузившись в содержимое, можно наткнуться на другие свидетельства, которые тоже могут довести до суда. В частности, самый обычный телефон может рассказать не только где вы были, но и что делали, благодаря чему полиция может узнать, не разговаривал ли водитель по телефону в момент аварии. Почти все смартфоны синхронизируются с каким-то сервером, и если даже вы удалили информацию на своём мобильном устройстве, то копия остаётся на сервере — либо у IT-отдела на работе, если вы используете BlackBerry, либо в iTunes, с которым вы синхронизируете iPhone. К сказанному остаётся добавить, что отнюдь не только власти желают получить доступ к секретам ваших телефонов.

Кстати, в феврале сотрудники Фраунгоферовского института технологий информационной защиты (Германия) наглядно продемонстрировали, что "извлечь" из iPhone или iPad с последней версией iOS сохранённые там пароли доступа к электронной почте и беспроводным сетям можно очень быстро. Даже если владелец устройства установил код, препятствующий несанкционированному использованию устройства, взлом всё равно не составляет особой трудности. В демонстрационном ролике, снятом в ходе эксперимента, процедура взлома iPhone 4, работающего под управлением iOS версии 4.2.1, "стандартным набором инструментов" заняла примерно 6 мин.

## К победе разума над здравым смыслом

Среди "благих намерений" по обеспечению кибербезопасности может скрываться всё, что угодно. Вот в июле было объявлено, что Вашингтон готов потратить 42 млн долл. на разработку ПО для выявления и систематизации данных о морально-психологическом состоянии военнослужащих и других групп населения разных стран, тенденциях и событиях, которые могут иметь отношение к безопасности США. Предполагается, что система будет отслеживать враждебную по отношению к США пропаганду и помогать вести контрпропаганду, используя подставных личностей, влияющих на онлайн-обсуждения и распространяющих американскую "точку зрения". Её название SMISC расшифровывается как "социальные медиа в стратегической коммуникации". Область развёртывания — Facebook, Twitter, YouTube и другие популярные социальные сервисы. Критики отмечают, что сам факт того, что американские военные разрабатывают механизм по созданию фальшивых онлайн-личностей (в Интернете их называют "ботами"), может привести к тому, что правительства других стран, частные компании и негосударственные компании захотят сделать что-то подобное. И тут лишь один шаг до появления нового вида киберпреступлений.

В соответствии с техзаданием каждая фальшивая онлайн-личность должна обладать правдоподобным прошлым и историей, и что любой из 50 управляющих личностями сможет оперировать фальшивыми онлайн-личностями со своих рабочих компьютеров "без страха быть раскрытыми хитрыми противниками". Существующие технологии уже позволяют вести секретную деятельность в блогах на иностранных языках, которая позволит противостоять экстремистам и вражеской пропаганде за пределами США. Онлайн-вмешательство планируется пока вести на четырёх языках: арабском, фарси, урду и пушту. Кстати, подобная система контроля онлайн-личности может быть подвержена уголовному преследованию, если будет использована против граждан США, где ряд людей-ботов уже предстали перед судом. Как правило, человечество расстаётся со своим прошлым смеясь. А потом, плача, встречает своё будущее.


тел. 608-83-05
Приём статей: mail@radio.ru
Вопросы: consult@radio.ru
РАДИО № 1, 2012