УДК 004.491.22

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ОСОБЕННОСТИ СОВРЕМЕННЫХ ВИРУСНЫХ УГРОЗ

Петрова Е. С., канд. эконом. наук,
доцент кафедры информационных систем в экономике и управлении,
Мордовский государственный университет имени Н. П. Огарёва, г. Саранск
Сидорова Ю. А., студентка 1 курса экономического факультета,
Мордовский государственный университет имени Н. П. Огарёва, г. Саранск

В статье рассмотрены некоторые аспекты обеспечения безопасности информационных систем, проведен анализ особенностей современных угроз безопасности.

Ключевые слова: информационные угрозы, информационная безопасность, троянские программы, фишинг

В современном мире информационные технологии играют значительную роль во всех сферах жизни человека. Представление современных областей производства, науки, спорта, экономики и культуры становится невозможным без применения компьютерных технологий. Компьютерные технологии в связи с тотальной компьютеризацией – приоритетный курс развития науки XXI века. Потребность в компьютерах возникает в повседневной жизни как при работе, научных исследованиях и образовании, так и при планировании досуга и реализации свободного времени.

Обратной стороной всех плюсов компьютерных технологий является их уязвимость. Уязвимость информации включает в себя подверженность информации воздействию различных дестабилизирующих факторов, которые могут привести к нарушению её конфиденциальности, целостности, доступности или неправомерному использованию, что, несомненно, пагубно складывается на правообладателе информации.

Вопросом первостепенной важности для пользователя становится проблема защищенности данных и системы, возможность безбоязненного использование принесенной извне информации и обеспечение стабильной работы компьютера. Особо остро проблема внешних угроз обнаруживается в связи с развитием Интернета, т.к. именно через него, зачастую, внедряются вирусы и вредоносные программы, которые появляются, модернизируются и заражают тысячи компьютеров ежедневно. Троянские программы (бэкдоры, руткиты, троянцы-вымогатели, блокировщики Windows), черви, вирусы, дозвонщики, программы-шпионы, фишиговые атаки – вот далеко не полный перечень неприятных сюрпризов, с которыми рано или поздно сталкивается незащищённый пользователь.

Угрозы безопасности информации подразделяются на активные и пассивные. Пассивные направлены в основном на несанкционированное использова-

ние информационных ресурсов информационных систем, не оказывая при этом влияния на её функционирование, прослушивание каналов связи и т.д. Активные угрозы имеют своей целью нарушение нормального функционирования информационных систем целенаправленного воздействия на её компоненты. К активным угрозам, например, относят вывод из строя компьютера или его операционной системы, искажение сведений в банке данных, разрушение программного обеспечения.

Компьютерная программа имеет своего автора и конкретное назначение, поэтому поведение вируса в системе задается его создателем (вирусописателем). Определение компьютерный вирус подразумевает под собой программу с функциями размножения собственных копий в файлах других программ. Обязательный атрибут, которым обладает компьютерный вирус – способность заражать собой другие файлы на компьютере. Компьютерные вирусы обладают способностью внедрять себя в «тело» других программ и файлов на компьютере в целях собственного размножения.

Первые компьютерные вирусы создавались своими авторами исключительно с целью самоутверждения - авторы пытались подтвердить собственные способности написанием данных программ. Зачастую никакого другого функционального применения, кроме самокопирования, вывода каких-либо сообщений шуточного характера, такие программы в себе не несли. Это лишь мешало работать на зараженной системе, но речи об уничтожении пользовательской информации в результате заражения таким компьютерным вирусом вовсе не шло. Позже вирусы стали обладать деструктивными функциями: удаляли на зараженной системе те или иные файлы пользователя, иногда и ряд системных файлов, что приводило операционную систему в негодность. Характерным для того периода являлся вирус WIN.CIH, который в определенный момент времени вызывал повреждение материнской платы компьютера, записывая в BIOS некорректную информацию.

Со временем число создаваемых компьютерных вирусов начало снижаться, отдавая пальму первенства троянским программам. Сегодня киберкриминал стал уделом профессионалов, имеющих целью своей деятельности получение прибыли. Из наиболее распространенных компьютерных вирусов последнего времени стоит отметить Sality и Virut (по классификации Лаборатории Касперского). Оба этих компьютерных вируса несут в себе четко выраженную экономическую составляющую, вовлекая зараженный компьютер в целую зомби-сеть, которая через Интернет может скрытно подчиняться своему хозяину (вирусописателю), рассылать спам или даже совершать DOS атаки на сервисы в сети Интернет. Фактически, глядя на компьютерный вирус Virut или Sality, мы сталкиваемся с трояном, дополненным способом размножения компьютерного вируса для пущей эффективности.

В качестве основных путей размножения первых компьютерных вирусов выступали дискеты для переноса информации, позже их сменили CD диски, после чего компьютерные вирусы начали активно размножаться уже через сеть Интернет. На сегодняшний день на просторах сети Интернет встретить компьютерный вирус куда сложнее, чем наткнуться на ту же троянскую программу

(троян). Очевидно, основным способом размножения компьютерных вирусов на сегодняшний день являются популярные сменные носители – USB Flash диски (флешки). На флешку компьютерный вирус может записаться самостоятельно, без участия пользователя.

Самое распространенное на сегодняшний день семейство вредоносных программ – троянские программы. Термин «троян» был заимствован из легендарной истории про троянского коня, благодаря которому в древности было совершено незаметное проникновение на территорию противника. Точно также и современные компьютерные трояны незаметно попадают в компьютер жертвы и начинают там своё скрытное существование. По сути, это всё те же вредоносные компьютерные программы, но лишенные возможности размножать свои копии через файлы других программ. Троян создается уже полностью готовым к работе. Компьютерные трояны обычно имеют своей целью шпионскую или воровскую деятельность, в ходе которой могут рассылать с зараженного компьютера спам, записывать и отправлять вводимую на клавиатуре информацию, собирать и воровать всевозможные пароли, осуществлять скрытное удаленное управление зараженным компьютером через Интернет и много другое.

Классификация троянских программ достаточно обширна. Сегодня можно встретить трояны-вымогатели, трояны для рассылки спама с зараженного компьютера (спамботы от англ. Spam bot), трояны для удаленного управления зараженным компьютером (бэкдоры от англ. backdoor), трояны для скрытной или обманной установки других троянов (дропперы), трояны для скрытной загрузки из интернета других троянских программ (даунлодеры). Так же стоит упомянуть трояны для кражи паролей с зараженного компьютера (например, паролей от программ-мессенджеров, социальных сетей, online игр и т.п.) и трояны для автоматического заражения компьютера через интернет. В последнее время достаточно популярны трояны, притворяющиеся антивирусными программами.

Наиболее распространены следующие виды троянских программ:

1.Клавиатурные шпионы (Trojan-SPY) – трояны, постоянно находящиеся в памяти и сохраняющие все данные поступающие от клавиатуры с целью последующей передачи этих данных злоумышленнику. Обычно таким образом злоумышленник пытается узнать пароли или другую конфиденциальную информацию.

2.Похитители паролей (Trojan-PSW) – трояны, также предназначенные для получения паролей, но не использующие слежение за клавиатурой. Обычно в таких троянах реализованы способы извлечения паролей из файлов, в которых эти пароли хранятся различными приложениями.

3.Утилиты удаленного управления (Backdoor) – трояны, обеспечивающие полный удаленный контроль над компьютером пользователя. Существуют легальные утилиты такого же свойства, но они отличаются тем, что сообщают о своем назначении при установке или же снабжены документацией, в которой описаны их функции. Троянские утилиты удаленного управления, напротив, никак не выдают своего реального назначения, так что пользователь и не по-

дозревает о том, что его компьютер подконтролен злоумышленнику. Наиболее популярная утилита удаленного управления - Back Orifice.

4. Анонимные smtp-сервера и прокси (Trojan-Proxy) – трояны, выполняющие функции почтовых серверов или прокси и использующиеся в первом случае для спам-рассылок, а во втором для заметания следов хакерами.

5. Модификаторы настроек браузера (Trojan-Cliker) – трояны, которые меняют стартовую страницу в браузере, страницу поиска или еще какие-либо настройки, для организации несанкционированных обращений к Интернет-ресурсам.

6. Инсталляторы прочих вредоносных программ (Trojan-Dropper) – трояны, предоставляющие возможность злоумышленнику производить скрытую установку других программ.

7. Загрузчики вредоносных программ (Trojan Downloader) – трояны, предназначенные для загрузки на компьютер-жертву новых версий вредоносных программ, или рекламных систем.

8. Уведомители об успешной атаке (Trojan-Notifier) – трояны данного типа предназначены для сообщения своему "хозяину" о зараженном компьютере.

9. "Бомбы" в архивах (ARCBomb) – трояны, представляющие собой архивы, специально оформленные таким образом, чтобы вызывать нештатное поведение архиваторов при попытке разархивировать данные – зависание или существенное замедление работы компьютера, заполнение диска большим количеством "пустых" данных.

10. Логические бомбы – чаще не столько трояны, сколько троянские составляющие червей и вирусов, суть работы которых состоит в том, чтобы при определенных условиях (дата, время суток, действия пользователя, команда извне) произвести определенное действие: например, уничтожение данных.

11. Утилиты дозвона – сравнительно новый тип троянов, представляющий собой утилиты dial-up доступа в Интернет через платные почтовые службы. Такие трояны прописываются в системе как утилиты дозвона по умолчанию и влекут за собой крупные счета за пользование Интернетом.

Уязвимости в модулях операционной системы способствуют заражению троянскими программами. Также представляют угрозу безопасности компьютера в плане заражения троянами уязвимости в вэб браузере и его плагинах (расширениях). Несмотря на то, что самый популярный среди пользователей браузер Internet Explorer постепенно сдает свои позиции, основной вектор атак злоумышленников направлен именно в сторону данного браузера. Для незаметного проникновения трояна через уязвимый браузер злоумышленники используют так называемые эксплойты – специальные коды данных, которые вызывают повреждение памяти и разрешают доступ к соседним её областям, что в конечном итоге позволяет заразить трояном компьютер. Уязвимость в плагинах браузеров связана с такими расширениями, как Adobe Flash Player для отображения FLASH анимации в браузере или Adobe Acrobat Reader для отображения PDF документов в браузере.

Для предотвращения заражения компьютера через Интернет необходимо пользоваться качественными антивирусными программами, оснащенными вэб

фильтрами. К числу качественных надежных антивирусов можно отнести лишь продукты двух российских компаний: Лаборатории Касперского и компании DRWeb.

Помимо скрытного заражения трояном, существует возможность открытого заражения троянской программой – сам пользователь фактически даёт злоумышленнику «зеленый свет», когда пользователю троян «предлагается» под видом чего-нибудь полезного. Методика введения пользователя в заблуждение путем сообщения ему важных для него данных, оказывающихся на самом деле ложными, в настоящее время испытывает очередной виток своего развития. Новых приемов пока не открыто, старые и давно испытанные используются в ужасающих масштабах. Одним из наиболее ярких примеров подобной методики являются фишинг-атаки. Фишинг – вид онлайнового мошенничества, цель которого – получить идентификационные данные пользователей. Организаторы фишинг-атак рассылают электронные письма от имени популярных брендов и вставляют в них ссылки на фальшивые сайты. Оказавшись на таком сайте, пользователь рискует сообщить преступникам ценную информацию, например, номер своей кредитной карты. Часто можно наткнуться на баннеры и всплывающие окна, имитирующие интерфейс операционной системы Windows. Когда хакеры пытаются установить вирус на чей-то компьютер, то в большинстве случаев им нужно, чтобы пользователь лично запустил программу. Чтобы убедить владельца компьютера сделать это, вирус, как правило, выдают за какое-то полезное программное обеспечение. Например, критическое обновление для Windows, антивирус, кодек, необходимый для просмотра видео на сайте, и т. д. Подделываясь под системные сообщения, баннеры «находят» в компьютере несуществующие вирусы и троянские программы, а затем предлагают установить некий антивирус, который на самом деле является, собственно, троянской программой. Таким образом, пользователя обманным путем вынуждают добровольно установить троян в свой компьютер, где-то играя на любопытстве, а где-то на невнимательности и страхе.

Стоит также упомянуть такие способы заражения троянскими программами, как системы обмена мгновенными сообщениями (ICQ, MSN Messenger и др.), а также электронную почту, с которой началась эпоха заражения компьютерными вирусами через Интернет (первые компьютерные вирусы начали освоение Сети именно через электронную почту посредством зараженных вложений в электронном письме). Сейчас такой способ размножения уже нельзя назвать популярным, поскольку антивирусные продукты и системы безопасности на почтовых серверах научились с завидным успехом находить и обезвреживать компьютерные вирусы и трояны в электронной почте. Вектор заражения троянами и вирусами через интернет сместился в сторону зараженных вэб-сайтов. По данным статистики антивирусных компаний, содержание вирусов и троянов в электронной почте сегодня находится на уровне 2-3 процентов от общего числа писем, что само по себе невелико. Но, тем не менее, электронную почту нельзя полностью снимать со счетов. Никогда не следует открывать и запускать вложения в электронных письмах от неизвестных отправителей. В последнее время злоумышленники стали вместо вложений в своих письмах

присылать ссылки на зараженный сайт, поэтому переходить по ссылкам в письмах от неизвестных отправителей также не рекомендуется. Что касается систем обмена мгновенными сообщениями, то здесь снова возможно столкнуться со ссылками на зараженные сайты, которую может прислать в своем сообщении один из контактов, чей компьютер в данный момент оказывается зараженным троянской программой, или же если номер и пароль клиента могли стать известны злоумышленникам.

Сменные носители также являются каналом, с помощью которого троянские программы попадают на компьютер: внешние жесткие диски, CD / DVD / Blu-Ray диски, флешки (USB Flash) и даже фотоаппараты, мобильные телефоны и MP3 плееры (т.к. информация в этих устройствах содержится в уязвлённой к вирусным программам картах памяти). Пик популярности этих устройств для заражения компьютера троянами приходится на последние 3 года. Самым распространенным вирусом уже длительное время является Conficker и его модификации, которые занимают сразу несколько мест в TOP 10 угроз, включая и первое. Они распространяются с помощью функции Autorun, запускающей исполняемый файл, прописанный в файле Autorun.inf при подключении внешнего накопителя к компьютеру. Этому способствовало и широкое распространение данных «девайсов», и уязвимость в операционных системах Windows (главным образом в Windows XP и Windows Vista), которая автоматически запускала троян на зараженной флешке при её подключении к компьютеру (благодаря информации из файла autorun.inf на сменном носителе). Файл autorun.inf создавался трояном для запуска своего исполняемого файла при подключении флешки к очередному компьютеру-жертве. Conficker копирует себя в систему, а затем на другие флеш-драйвы и винчестеры, подсоединяемые к компьютеру. Чаще всего сам вирус используется для организации ботнет-сетей. Вероятно, именно в связи с его эпидемией Microsoft недавно отключила функцию Autorun в Windows XP/Vista с помощью обновления, выпущенного в начале февраля этого года. В Windows 7 автозапуск неактивен по умолчанию.

В случае с компьютерными вирусами и троянами - не допустить заражения всегда проще, чем в дальнейшем проводить долгое и трудоемкое лечение вирусов. Сегодня популярные антивирусы последних версий уделяют проблеме безопасности сменных носителей особое внимание и предлагает провести проверку на вирусы перед запуском или открытием содержимого флешки. Контроль над чужим ПК позволяет создавать ботнет-сети, в состав которых иногда входят сотни тысяч компьютеров. Такие виртуальные армии формируются для рассылки спама или DDOS-атак на сайты. Пользователи зачастую даже не подозревают о том, что их ПК управляет кто-то другой.

Помимо кражи банковских и платежных данных пользователей, вирусописатели не обходят вниманием еще одну черту современного интернета - все возрастающую популярность различных онлайновых игр. Современный рынок онлайновых игр, появившийся с выходом в 1997 году MMORPG Ultima Online, сейчас переживает период своего максимального расцвета и, скорее всего, будет активно развиваться и в будущем. На интернет-аукционах стоимость предметов или игровых персонажей для какой-либо игры может достигать несколь-

ких десятков тысяч долларов. Известен случай, когда «виртуальный остров» в одной из таких игр был продан за 26500 долларов. Общий оборот денег, так или иначе задействованных в различных «игровых вселенных», уже составляет несколько миллиардов долларов, приближаясь к бюджету небольшого государства. Рост популярности онлайновых игр и объема задействованных в них денег не могли не привлечь внимания злоумышленников.

Рассмотрим некоторые особенности угроз информационной безопасности, зафиксированных в 2010 году, который можно назвать годом расцвета интернет-мошенничества.

1. Банковские троянцы. Первое место в списке кибер-вредителей присуждается банковским троянцам. К данной категории вредоносных программ относятся те из них, которые ориентированы на получение неавторизованного доступа злоумышленников к счетам физических и юридических лиц посредством систем дистанционного банковского обслуживания. Последние сейчас стремительно набирают популярность, и преступники стремятся этой популярностью воспользоваться. Вероятно, в 2011 году мы станем свидетелями смещения сферы интересов интернет-мошенников с частных пользователей на юридических лиц, на счетах которых сосредоточены куда более значительные суммы денег.

PandaLabs представила свой ежегодный отчёт вирусной активности. Самым популярным типом вирусов этого года оказались трояны. Аналитики отмечают, что в 2010 году количество созданных и распространенных кибермошенниками вирусов составило 1/3 всех когда-либо существовавших вирусов. Так называемые, банковские трояны доминируют в рейтинге новейшего вредоносного ПО, которое появилось в 2010 году (56% всех новых образцов). На втором месте по «популярности» находятся вирусы и черви. Список наиболее инфицированных стран возглавили Таиланд, Китай, Тайвань, Украина и Латвия с показателем инфицированности в пределах 50-70%.

2. Блокировщики Windows. Второе место по праву занимают классические блокировщики Windows, которые держат в напряжении пользователей и специалистов антивирусных компаний с осени 2009 года. К блокировщикам Windows относят вредоносные программы, которые выводят окно (блокирующее другие окна) с требованиями злоумышленников. Таким образом, пользователь лишается возможности работать за компьютером, пока не заплатит за разблокирование. Разнообразие таких блокировщиков, как и предлогов мошенников шокирует – от требований заплатить штраф за использование пиратского ПО до требований оплаты заказанного порно-контента.

3. Шифровальщики данных. В 2010 году появилось множество новых модификаций троянцев-шифровальщиков, целью которых являются документы пользователей. После того как троянец зашифровывает документы, выводится информация о том, что за расшифровку необходимо отправить деньги злоумышленникам. В подавляющем большинстве случаев вирусологи оперативно разрабатывают утилиты, с помощью которых можно расшифровать пользовательские данные, но, поскольку это возможно не всегда и злоумышленники

требуют за расшифровку значительные суммы денег, Trojan.Encoder занимает третью строчку нашей десятки.

4. Редиректоры на вредоносные и мошеннические сайты. Данные вредоносные программы создаются злоумышленниками для изменения системного файла hosts таким образом, чтобы при попытке зайти на популярный сайт (например, одной из популярных социальных сетей) в интернет-браузере отображался фальшивый сайт с дизайном, похожим на оригинальный. Обычно блокируется доступ к большинству поисковых систем, дабы лишить пользователя возможности самостоятельно «расправиться» с вирусом. При этом с пользователя под разными предлогами будут требоваться деньги. Самые популярные требования мошенников такие: пользователь должен отправить СМС для разблокирования доступа к социальной сети; пользователь должен оправить СМС для подтверждения того, что он не является ботом; и.т.п. При этом некоторые вирусы меняют в реестре путь к файлу hosts, таким образом, уменьшая вероятность того, что среднестатистический пользователь самостоятельно справится с вредоносом.

5. Лжеантивирусы. Лжеантивирусы внешне похожи на антивирусное ПО, и часто их дизайн напоминает сразу несколько антивирусных продуктов. Но ничего общего с антивирусами эти вредоносные программы не имеют. Будучи установленными в систему, такие «антивирусы» сразу же сообщают о том, что система якобы заражена (отчасти это соответствует истине), и для лечения системы якобы необходимо приобрести платную версию антивирусной программы. В некоторых случаях угрожают удалить всю информацию с жесткого диска или привести компьютер в негодность.

6. Блокировщики запуска IM-клиентов. На протяжении нескольких месяцев в 2010 году злоумышленники распространяли вредоносную программу, которая блокировала запуск популярных клиентов мгновенного обмена сообщениями. Под ударом оказались пользователи ICQ, QIP и Skype. IM-клиент заменялся похожим по интерфейсу вредоносным ПО, в котором при запуске пользователю сообщалось, что его учётная запись заблокирована за рассылку спама, а за восстановление доступа к соответствующему сервису необходимо отправить СМС-сообщение, естественно, на платный номер.

7. Ложные архивы. Злоумышленниками придумано и воплощено десятки схем получения нелегального дохода, а само вредоносное ПО попало на сотни миллионов компьютеров.

На такое окно хотя бы раз в жизни наталкивались практически все пользователи Интернет. Злоумышленники создают поддельные (fake) торрент-трекеры или файловые хранилища, с которых якобы можно скачать популярный или редкий контент. Данные ресурсы появляются в первых строчках популярных запросов в поисковых системах. Воспользовавшись таким ресурсом, жертва получает к скачиванию якобы самораспаковывающийся архив, в котором имеется желанная информация. В реальности «архив» оказывается исполняемым файлом (*.exe), интерфейс и иконка очень похожа на самораспаковывающийся архив. Отличие такого архива от настоящего заключается в том, что в процессе «распаковки» в определенный момент пользователю выводится ин-

формация о том, что для окончания процесса необходимо выплатить некоторую сумму денег. Фактически пользователь обманывается дважды — отправляет деньги злоумышленникам и не получает никакой полезной для себя информации. Архивы не содержат в себе ничего, кроме визуальной оболочки и мусора, а их размер (видимо, для усыпления бдительности пользователей) может достигать 70 МБ и более.

8. Загрузочные блокировщики

В ноябре 2010 года зафиксировано распространение блокировщика, который при заражении прописывается в загрузочную область жесткого диска, тем самым блокируя загрузку используемой операционной системе. При включении компьютера на экран пользователя выводится информация с требованиями злоумышленников. Разработчики конкретно этого «вредоноса» требуют за ключ $100.

Что касается наиболее популярных методов инфицирования, то в 2010 году ими стали: распространение вредоносного ПО с помощью социальных сетей, создание поддельных сайтов (атаки BlackHat SEO); использование так называемых уязвимостей «нулевого» дня.

В течение 2010 года продолжал активно распространялся спам, даже несмотря на то, что были ликвидированы некоторые бот-сети (например, *Mariposa* и *Bredolad*). Это уберегло миллионы компьютеров от угрозы и, конечно, повлияло на общемировой спам-траффик. В 2009 году примерно 95% всех электронных писем оказывались спамом, однако в 2010 году этот показатель снизился примерно до 85%.

2010 год можно назвать годом год кибер-преступности и кибер-войн. В прошедшем году мы видели несколько примеров кибер-войн. Одна из самых ярких подобных войн была вызвана червем Stuxnet. Ему удалось инфицировать атомную электростанцию вблизи города Бушер (Иран), что подтвердили иранские власти.

Еще одна яркая кибер-война 2010 года – «Операция Аврора». Целью этой атаки стали работники некоторых крупных транснациональных корпораций. Их рабочие компьютеры были инфицированы Трояном, который способен получить доступ ко всей конфиденциальной информации.

2010 год также продемонстрировал нам появление нового явления, навсегда изменившего отношения между обществом и сетью Интернет: кибер-протесты или, так называемый, хактивизм. Этот феномен стал известен благодаря «Анонимной группе». На самом деле, он не является чем-то абсолютно новым, однако в этот раз о нём писали все издания. «Анонимная группа» организовала множественные DDoS-атаки, которые обрушили системы сайтов различных обществ защиты авторского права. Таким образом, эта группа стремилась защитить основателя сайта Wikileaks Джулиана Ассанджа.

Анализируя все вышесказанное, можно заключить, что в условиях значительного усиления противодействия вирусным атакам и существенного роста пользовательской грамотности в области противостояния интернет-угрозам, вирусописатели и хакеры вынуждены активно развивать методы социального

инжиниринга, позволяющие проникнуть даже на самый защищенный пользовательский компьютер.

INFORMATION SECURITY: SINGULARITIES OF THE MODERN VIRUS THREATS

Petrova E. S., PhD, Associate Professor, the chair of information systems in economics and management, Ogarev Mordovia State University, Saransk
Sidorova U. A., the 1st year student of Department of Economics, Ogarev Mordovia State University, Saransk

In article some aspects of safety of information systems are considered, the analysis of singularities of the modern security risks is carried out

Keywords: information threats, information security, Trojan programs, phishing