УДК 004.491.22

Нуянзин А.Ю.,
студент 3 курса
Средне–Волжский институт (филиал) ВГУЮ (РПА Минюста России)
г.Саранск

ТРОЯНСКАЯ ПРОГРАММА КАК ОДНА ИЗ ОСНОВНЫХ УГРОЗ ИНФОРМАЦИИ ПОЛЬЗОВАТЕЛЯ

Аннотация: *В статье рассматривается проблема заражения компьютеров пользователей вредоносным ПО «Троян». Раскрываются основные признаки данной программы и выявляются отличительные особенности Троянской программы. Предлагаются средства защиты компьютера.*

Ключевые слова: *вирус, вредоносная программа, хакер, вирусная атака, вирусная диверсия.*

Annotation: *The article deals with the problem of infecting users' computers with Trojan malicious software. The main features of this program are revealed and the distinctive features of the Trojan program are revealed. Computer protection is offered.*

Key words*: virus, malware, hacker, virus attack, virus diversion.*

Мы живем во время, в которое с каждым днем научно-технический прогресс делает огромный шаг вперед. Это достигается благодаря успехам и открытиям в различных областях науки. Ежедневно из средств массовой информации мы видим, что значительную часть работы за человека выполняет искусственный интеллект, созданный для того, чтобы облегчить труд людей, сделать его более продуктивным и исключить возможность ошибки. Последнее, к сожалению, не всегда получается осуществить, поэтому и в настоящее время ведутся исследования в области компьютерных

технологий. Роботы выполняют за человека сложнейшие вычисления, управляют беспилотными самолетами, проводят хирургические операции (в том числе операции на роговице глаза), помогают в освоении космоса и т.д. Но у медали есть и вторая сторона. Очень часто такие технологии используются в корыстных целях, для : незаконного завладения имуществом человека, доступа к конфиденциальной информации, взлома системы безопасности с целью облегчения совершения преступления и т.д. Одним из самых громких случаев кибератак являются действия преступников-хакеров, которые происходили в 2012 году. 21 декабря злоумышленники смогли снять в 4 тысячах банкоматах 5 миллионов долларов. Они получили доступ к индийскому оператору предоплаченных карт Visa и MasterCard, перекодировали карты в 20 странах мира. Спустя 2 месяца ущерб от их действий уже составлял 40 миллионов долларов. В конце 2008 года в сети обнаружили вирус — Conficker. Но было слишком поздно, потому что через 4 месяца он проник уже в 12 миллионов компьютеров. В результате действий этого вируса пострадали цифровые системы британских военно-морских сил и Палата общин британского парламента [1]. Перечислять можно бесконечно, но ясно одно — во всех случаях, действия таких программ носят деструктивный и разрушающий характер. Сегодня под компьютерным вирусом понимается один из видов программного обеспечения, который имеет способность создавать копии самого себя и может внедряться в код других программ, в области памяти, распространять свой код по различным каналам связи[2].

На сегодняшний день существует огромное количество вирусных программ, но одним из самых опасных вирусов эксперты считают «Троян». Название обусловлено важной исторической вехой. Во время Троянской войны спартанцы очень долго не могли взять крепость Трои. После многих неудачных попыток спартанцы решили захватить Трою хитростью. Они соорудили огромного деревянного коня, внутри которого находились 50

лучших спартанских воинов. Этого коня они оставили у ворот Трои. Гарнизон крепости воспринял это как подарок и принесение извинений со стороны нападающих и ,ничего не заподозрив, взял этого коня в крепость. Дождавшись ночи, воины Спарты вылезли из коня и перебили стражу, неприступная крепость пала. Это название дано вирусу не просто так, а в силу его особенных свойств. В отличии от других вредоносных программ Троян проникает в компьютер не при помощи атаки на технику, а путем диверсии. Пользователь может и вовсе не знать о том, что его компьютер инфицирован до тех пор, пока вирус не начнет свою деятельность внутри системы. Опасность также состоит в том, что сейчас большинство таких вирусов создаются для работы в интернете ,и к пользователю он может попасть совершенно случайно, например при скачивании «полезного» файла, каких-либо документов. Одним из самых главных отличий Трояна от других вирусов является то, что после активации он продолжает поддерживать связь со своим создателем, в то время как другие начинают существовать самостоятельно. Когда Троян попадает на компьютер пользователя, он начинает свою диверсионную деятельность. Хакер легко может получить доступ ко всей информации, хранящейся на компьютере человека, может установить серверы дистанционного управления и работать на своем компьютере от имени его «жертвы». Злоумышленник может не только просматривать информацию пользователя, но и совершать различные операции: передавать, копировать, удалять, изменять и т.д. Когда подобный вирус попадает на компьютер, первое, что ему необходимо сделать — надежно закрепиться в системе. Одним из самых частых мест нахождения Трояна является реестр. Реестр — это сложная область, база данных, которая хранит различные настройки и параметры операционной системы, настройки программ и компонентов, установленных на компьютере. В этом-то и заключается опасность — вирус получает фактически безграничную возможность манипуляции информацией и распоряжение ею по своему

усмотрению, а вернее, по усмотрению злоумышленника, создавшего эту программу. Вторым местом, в котором может храниться троянская программа является папка «Автозагрузка». В этой папке можно найти программы, которые начинают запускаться ,как только операционная система начинает работу. Поэтому человек, не зная того, что на его компьютере находится вирус, запустив операционную систему, параллельно может запустить вирус. В зависимости от функций Троянов, выделяют следующие их разновидности:

1. Бэкдор — способна предоставлять злоумышленнику возможность управления компьютером пользователя. Т.е. хакер может выполнять различные действия на компьютере пользователя: отправка, удаление, открытие, получение различных файлов.
2. Эксплойт — вирус, использующий приложения, работающие на компьютере.
3. Руткит — может скрыть в системе некоторые объекты. Используется для того, чтобы скрыть вирус от обнаружения.
4. Банковские троянцы — предназначены для кражи учетных данных систем интернет-банкинга, систем электронных платежей и кредитных или дебетовых карт.
5. DDoS-троянцы — занимаются проведением атак по веб-адресам. В процессе данной атаки с инфицированных компьютеров людей отправляется огромное количество запросов, что вызывает перегрузку системы.
6. Trojan-FakeAV — занимаются имитацией работы антивирусного программного обеспечения. Создаются для того, чтобы вымогать деньги у пользователей в обмен на обнаружение угроз и вредоносных ПО [3].

Для того, чтобы защититься от троянских программ необходимо просканировать реестр, воспользовавшись специальными утилитами.

Эксперты советую проверять и папку «Автозагрузки», для того, чтобы исключить вероятность систематичного запуска вируса с каждой загрузкой операционной системы. Также необходимо использовать надежные антивирусные программы, которые обеспечивают защиту не только от локальных вирусов, но и от вэб-угроз.

Использование антивирусного ПО также не наделит пользователя 100% гарантией того, что его компьютер не будет инфицирован т.к. ежедневно создается около 10000 различных вирусов и создателям антивирусов необходимо немало времени, чтобы выявить новые угрозы, понять принцип их действия и принцип заражения, а уже потом разработать защиту. Поэтому специалисты советуют создавать резервные копии системы, использовав соответствующее ПО, чтобы в необходимых ситуациях восстановить прежнюю работу системы.

Библиографический список

1. РИА Новости. Электронный ресурс. Режим доступа — https://ria.ru

2. IT-Журнал. Электронный ресурс. Режим доступа — http://iteranet.ru

3. Лаборатория Касперского. Электронный ресурс. Режим доступа — https://www.kaspersky.ru