ВРЕДОНОСНЫЕ ПРОГРАММЫ И ИХ КЛАССИФИКАЦИЯ. ОСНОВНЫЕ КАНАЛЫ РАСПРОСТРАНЕНИЯ КОМПЬЮТЕРНЫХ ВИРУСОВ И ДРУГИХ ВРЕДОНОСНЫХ ПРОГРАММ

Баран М.Л., Санкевич Н.А.
Научный руководитель: ст. преподаватель Ковалькова И.А.
Белорусский национальный технический университет

Массовое применение персональных компьютеров, к сожалению, оказалось связанным с появлением самовоспроизводящихся программ-вирусов, препятствующих нормальной работе компьютера, разрушающих файловую структуру дисков и наносящих ущерб хранимой в компьютере информации. Несмотря на принятые во многих странах законы о борьбе с компьютерными преступлениями и разработку специальных программных средств защиты от вирусов, количество новых программных вирусов постоянно растет. Это требует от пользователя персонального компьютера знаний о природе вредоносных программ, способах заражения вирусами и защиты от них.

Вредоносная программа (англ. *malware*: словослияние слов ***mal****icious* и *soft****ware***) – любое программное обеспечение, предназначенное для получения несанкционированного доступа к вычислительным ресурсам самой ЭВМ или к информации, хранимой на ЭВМ, с целью несанкционированного использования ресурсов ЭВМ или причинения вреда (нанесения ущерба) владельцу информации, и/или владельцу ЭВМ, и/или владельцу сети ЭВМ, путём копирования, искажения, удаления или подмены информации.

Классификация вредоносных программ:

1. *Агенты ботнетов*. Ботнетом называется группа заражённых компьютеров, получающих команды от злоумышленника; за приём и исполнение этих команд отвечает соответствующая вредоносная программа. Такая сеть может насчитывать от нескольких единиц до миллионов компьютеров, она также называется зомби-сетью.

2. *Эксплойт* – теоретически безобидный набор данных (например, графический файл или сетевой пакет), некорректно воспринимаемый программой, работающей с такими данными. Здесь вред наносит не сам файл, а неадекватное поведение ПО с ошибкой, приводящее к уязвимости. Также эксплойтом называют программу для генерации «отравленных» данных.

3. *Бекдоры* – программы для удалённого подключения к компьютеру и управления им.

4. *Сетевые черви* – вредоносные программы с самой разной функциональной нагрузкой, которые способны самостоятельно распространяться по компьютерным сетям.

5. *Логическая бомба* – вредоносная часть компьютерной программы (полезной или нет), срабатывающая при определённом условии.

6. *«Троянские кони» («трояны»)* – широкий класс вредоносных объектов разнообразного назначения, которые обычно не имеют собственного механизма распространения (т.е. не могут заражать файлы или размножать свои копии через сеть). Название произошло от ранней тактики их проникновения – под видом легитимной программы или в качестве скрытого дополнения к ней. Вредоносное ПО может образовывать цепочки: например, с помощью эксплойта на компьютере жертвы развёртывается загрузчик, устанавливающий из интернета червя-вирус с логическими бомбами.

Для того чтобы создать эффективную систему антивирусной защиты компьютеров и корпоративных сетей, необходимо чётко представлять себе, откуда грозит опасность. Вирусы находят самые разные каналы распространения, причём к старым способам постоянно добавляются новые.

Классические способы распространения компьютерных вирусов

Файловые вирусы распространяются вместе с файлами программ в результате обмена дискетами и программами, загрузки программ из сетевых каталогов, с Web- или ftp-серверов. *Загрузочные вирусы* попадают на компьютер, когда пользователь забывает заражённую дискету в дисководе, а затем перезагружает ОС. Загрузочный вирус также может быть занесён на компьютер вирусами других типов. *Макрокомандные вирусы* распространяются в результате обмена заражёнными файлами офисных документов, такими как файлы Microsoft Word, Excel, Access.

Если заражённый компьютер подключён к локальной сети, вирус легко может оказаться на дисках файл-сервера, а оттуда через каталоги, доступные для записи, попасть на все остальные компьютеры сети. Так начинается вирусная эпидемия. Системному администратору следует помнить, что вирус имеет в сети такие же права, что и пользователь, на компьютер которого этот вирус пробрался. Поэтому он может попасть во все сетевые каталоги, доступные пользователю. Если же вирус завёлся на рабочей станции администратора сети, последствия могут быть очень тяжёлыми.

Электронная почта

В настоящее время глобальная сеть Internet является основным источником вирусов. Большое число заражений вирусами происходит при обмене письмами по электронной почте в форматах Microsoft Word. Электронная почта служит каналом распространения макрокомандных

вирусов, так как вместе с сообщениями часто отправляются офисные документы.

Заражения вирусами могут осуществляться как непреднамеренно, так и по злому умыслу. Например, пользователь заражённого макровирусом редактора, сам того не подозревая, может рассылать заражённые письма адресатам, которые в свою очередь отправляют новые заражённые письма. С другой стороны, злоумышленник может преднамеренно послать по электронной почте вместе с вложенным файлом исполняемый модуль вирусной или троянской программы, вредоносный программный сценарий Visual Basic Script, заражённую или троянскую программу сохранения экрана монитора, словом – любой опасный программный код.

Распространители вирусов часто пользуются для маскировки тем фактом, что диалоговая оболочка Microsoft Windows по умолчанию не отображает расширения зарегистрированных файлов. Например, файл с именем FreeCreditCard.txt.exe, будет показан пользователю как FreeCreditCard.txt. Если пользователь попытается открыть такой файл, будет запущена вредоносная программа.

Сообщения электронной почты часто приходят в виде документов HTML, которые могут включать ссылки на элементы управления ActiveX, апплеты Java и другие активные компоненты. Из-за ошибок в почтовых клиентах злоумышленники могут воспользоваться такими активными компонентами для внедрения вирусов и троянских программ на компьютеры пользователей. При получении сообщения в формате HTML почтовый клиент показывает его содержимое в своём окне. Если сообщение содержит вредоносные активные компоненты, они сразу же запускаются и выполняют заложенные в них функции. Чаще всего таким способом распространяются троянские программы и черви.

Троянские Web-сайты

Пользователи могут «получить» вирус или троянскую программу во время простого серфинга сайтов Интернета, посетив троянский Web-сайт. Ошибки в браузерах пользователей зачастую приводят к тому, что активные компоненты троянских Web-сайтов (элементы управления ActiveX или апплеты Java) внедряют на компьютеры пользователей вредоносные программы. Здесь используется тот же самый механизм, что и при получении сообщений электронной почты в формате HTML. Но заражение происходит незаметно: активные компоненты Web-страниц могут внешне никак себя не проявлять. Приглашение посетить троянский сайт пользователь может получить в обычном электронном письме.

Локальные сети

Локальные сети также представляют собой путь быстрого заражения. Если не принимать необходимых мер защиты, то заражённая рабочая

станция при входе в локальную сеть заражает один или несколько служебных файлов на сервере. В качестве таких файлов могут выступать служебный файл LOGIN.COM, Excel-таблицы и стандартные документы-шаблоны, применяемые в фирме. Пользователи при входе в эту сеть запускают заражённые файлы с сервера, и в результате вирус получает доступ на компьютеры пользователей. [1]

Другие каналы распространения вредоносных программ

Одним из серьёзных каналов распространения вирусов являются пиратские копии ПО. Часто нелегальные копии на дискетах и CD-дисках содержат файлы, заражённые разнообразными типами вирусов. К источникам распространения вирусов следует также отнести электронные конференции и файл-серверы ftp и BBS. Часто авторы вирусов закладывают заражённые файлы сразу на несколько файл-серверов ftp/BBS или рассылают одновременно по нескольким электронным конференциям, причём заражённые файлы обычно маскируют под новые версии программных продуктов и даже антивирусов. Компьютеры, установленные в учебных заведениях и Интернет-центрах и работающие в режиме общего пользования, также могут легко оказаться источниками распространения вирусов. Если один из таких компьютеров оказался заражённым вирусом с дискеты очередного пользователя, тогда дискеты и всех остальных пользователей, работающих на этом компьютере, окажутся заражёнными. [2]

По мере развития компьютерных технологий совершенствуются и компьютерные вирусы, приспосабливаясь к новым для себя сферам обитания. В любой момент может появиться компьютерный вирус, троянская программа или «червь» нового, неизвестного ранее типа, либо известного типа, но нацеленного на новое компьютерное оборудование. Новые вирусы могут использовать неизвестные или не существовавшие ранее каналы распространения, а также новые технологии внедрения в компьютерные системы. Чтобы исключить угрозу вирусного заражения, системный администратор корпоративной сети должен внедрять методики антивирусной защиты и постоянно отслеживать новости в мире компьютерных вирусов.

Литература

1. Н.Н.Безруков "Классификация компьютерных вирусов MS-DOS и методы защиты от них", Москва, СП "ICE", 1990 г.

2. Дата центр// [Электронный ресурс]. – Режим доступа: (https://studref.com/322543/informatika/.osnovnye_kanaly_rasprostraneniya_virusov_drugih_vredonosnyh_programm)/ Дата доступа: 26.03.2021.