Содержание

Введение

В настоящее время компьютеры осуществляют огромное количество целей и задач. С каждым днём растёт количество пользователей электронно-вычислительных систем. Это ведёт к стремительному развитию вредоносного программного обеспечения.

Цель данной работы – ознакомиться с определением вредоносного ПО, рассмотреть его разновидности и способы защиты.

Определение вредоносного программного обеспечения

Вредоносное программное обеспечение – это любое программное обеспечение, предназначенное для осуществления несанкционированного доступа и/или воздействия на информацию или ресурсы информационной системы в обход существующих правил разграничения доступа**.**

К разновидностям вредоносного ПО относятся:

- Вирусы
- Черви
- Клавиатурные шпионы
- Загрузочные вирусы
- Программы для кражи паролей
- Трояны
- Вредоносные утилиты
- Рекламные программы
- Шпионские программы

Проблема вредоносных программ – заслуживает повышенного внимания как одна из самых главных неприятностей, с которыми ежедневно сталкиваются современные пользователи компьютеров. Их пагубное воздействие проявляется в том, что они подрывают принцип надёжности компьютера и нарушают неприкосновенность личной жизни, нарушают конфиденциальность и разрывают отношения между защищёнными механизмами работы компьютера, посредством некоторых комбинаций шпионских действий. Подобные программы часто появляются без ведома

получателя, и даже при обнаружении от них трудно избавиться. Заметное снижение производительности, беспорядочная смена пользовательских настроек и появление новых сомнительных панелей инструментов являются лишь немногими страшными последствиями заражения вредоносной программой. Вредоносные программы могут также прилаживаться к более незаметным режимам функционирования компьютера и глубоко внедряться в сложные механизмы работы операционной системы так, чтобы в значительной степени осложнить их обнаружение и уничтожение.

Разновидности вредоносного программного обеспечения

3.1 Компьютерные вирусы

Компьютерные вирусы – это разновидность вредоносного ПО, которое способно копировать себя и распространяться на другие компьютеры. Вирусы часто распространяются на другие компьютеры, присоединяясь к различным программам и выполняя код, когда пользователь запускает одну из этих зараженных программ. Вирусы также могут распространяться через файлы сценариев, документы и уязвимости межсайтового сценария в веб-приложениях. Вирусы можно использовать для кражи информации, нанесения вреда хост-компьютерам и сетям, создания бот-сетей, кражи денег, отображения рекламы и многого другого.

При заражении компьютера вирусом важно его обнаружить, для этого следует знать основные признаки его проявления:

- прекращение работы или неправильная работа ранее успешно функционировавших программ;
- медленная работа компьютера;
- невозможность загрузки операционной системы;
- исчезновение файлов и каталогов или искажение их содержимого;
- изменение даты и времени модификации файлов;
- изменение размера файлов;
- неожиданное значительное увеличение количества файлов на диске;
- существенное уменьшение размера свободной оперативной памяти;

- вывод на экран непредусмотренных сообщений или изображений;

- подача непредусмотренных звуковых сигналов;

- частые зависания и сбои в работе компьютера.

Попав в среду компьютера, вирус может и не вызвать довольно серьезных последствий (например, ограничиться безобидными визуальными или звуковыми эффектами), а может уничтожить или изменить данные, также эта информация может стать «достоянием общественности».

Но есть вариант и похуже: в худшем случае компьютер станет неисправным, и контролировать его сможет только создатель вируса. Также стоит отметить, что вредоносные программы обычно занимают некоторое место, порой довольно большую часть оперативной памяти или накопителя информации.

3.2 Черви

Черви — это разновидность вирусов, которые проникают в компьютер без вмешательства пользователя. Черви эксплуатируют уязвимости программного обеспечения, чтобы проникнуть во внутреннюю среду компьютера. Именно эти слабые места программного обеспечения дают машинному коду возможность загрузиться, так вирус-червь оказывается в операционной системе и начинает заражать другие компьютеры посредством локальной или глобальной сети. Чаще всего такой вирус используется для рассылки спама или для DDoS-атак (вирусные атаки, цель которых заключается в выведении компьютера из строя).

Способы распространения:

- в виде файла, отправленного во вложении в электронном письме;

- в виде ссылки на интернет-сайт или FTP-ресурс

- в виде ссылки, переданной через сообщение

- через пиринговые сети обмена данными P2P

- некоторые черви распространяются как сетевые пакеты. Они проникают прямо в компьютерную память, затем активируется код червя.

Для защиты от данного типа вредоносного ПО необходимо чаятельно проверять источники ссылок и файлов, а также установить и настроить на компьютере брандмауэр.

3.3 Троянские программы

Троянские программы – это вредоносные программы, внешне выглядящие как легальный программный продукт, но при запуске осуществляющие несанкционированные действия, направленные на уничтожение, блокирование, модификацию или копирование информации, нарушение работы компьютеров или компьютерных сетей. В отличие от вирусов и червей, представители данной категории не имеют способности создавать свои копии, обладающие возможностью дальнейшего самовоспроизведения.

Троянская программа стягивает свои модули в одно место под модули действующих программ, создавая файлы со схожими названиями и характеристиками, меняет записи в системном реестре, изменяя ссылки рабочих модулей программ на свои, вызывающие модули вируса

К данной категории вредоносных программ относятся:

- Backdoor (бэкдор) – вредоносная программа, предназначенная для скрытого удалённого управления злоумышленником пораженного компьютера. По своей функциональности бэкдоры во многом напоминают

различные системы администрирования, разрабатываемые и распространяемые фирмами-производителями программных продуктов. Эти вредоносные программы позволяют делать с компьютером всё, что в них заложил автор: принимать или отсылать файлы, запускать и уничтожать их, выводить сообщения, стирать информацию, перезагружать компьютер и т.д.

Представители данного типа вредоносных программ очень часто используются для объединения компьютеров-жертв в так называемые ботнеты, централизованно управляемые злоумышленниками в злонамеренных целях. Botnet (ботнет) – это компьютерная сеть, состоящая из некоторого количества хостов, с запущенными ботами – автономным программным обеспечением. Чаще всего бот в составе ботнета является программой, скрытно устанавливаемой на компьютере жертвы и позволяющей злоумышленнику выполнять некие действия с использованием ресурсов заражённого компьютера.

Отдельно следует отметить группу бэкдоров, способных распространяться по сети и внедряться в другие компьютеры, как это делают сетевые черви. Отличает такие бэкдоры от червей то, что они распространяются по сети не самопроизвольно (как сетевые черви), а только по специальной команде "хозяина", управляющего данной копией троянской программы.

- Exploit (эксплойт) – программы, в которых содержатся данные или исполняемый код, позволяющие использовать одну или несколько уязвимостей в программном обеспечении на локальном или удаленном компьютере с заведомо вредоносной целью. Обычно эксплойты используются злоумышленниками для проникновения на компьютер-жертву с целью последующего внедрения туда вредоносного кода (например, заражение вредоносной программой всех посетителей взломанного Web-сайта).

- Rootkit – программа, предназначенная для сокрытия в системе определенных объектов либо активности. Сокрытию, как правило, подвергаются ключи реестра (например, отвечающие за автозапуск вредоносных объектов), файлы, процессы в памяти зараженного компьютера, вредоносная сетевая активность. Сам по себе Rootkit ничего вредоносного не делает, но данный тип программ в подавляющем большинстве случаев используется вредоносными программами для увеличения собственного времени жизни в пораженных системах в силу затрудненного обнаружения.

Для защиты от данного типа вредоносных программ необходимо использовать только лицензионное программное обеспечение, а также не устанавливать программы из непроверенных источников.

3.4 Логические бомбы

Логическая бомба – это вредоносное ПО, которое активируется ответом на какое-либо событие — например, запуск пользователем приложения, посещение целевого веб-сайта или по наступлению определенной даты (в таком случае называется «временной бомбой»).

Есть два основных типа логических бомб:

- Первый — когда логическая бомба интегрирована в вирусный комплекс, например, с трояном и клавиатурным шпионом. Пользователь сначала скачивает троян, который устанавливает клавиатурный шпион и логическую бомбу. Как только жертва заходит на нужный сайт, где требуется ввести личные данные (логин, пароль, номер карты и пр.), логическая бомба запускает клавиатурный шпион, а тот в свою очередь считывает нажатия клавиш и отправляет информацию заказчику.

- Второй тип логических бомб — встроенный в официальную программу код, который запускается по заложенному разработчиком сценарию. Из недавних примеров — нашумевшее дело с программистом-подрядчиком Siemens, Дэвидом Тинли, которого осудили за мошенничество с логической бомбой. Программист разрабатывал сложноустроенные таблицы Excel, с помощью которых компания решала часть своих CRM-задач. Таблицы в определенный момент начинали работать с ошибками, и Siemens ничего не оставалось делать, как обращаться за платным сервисом к Тинли. В итоге программиста обвинили в умышленном саботаже.

Для защиты от логической бомбы необходимо использовать только лицензионное программное обеспечение, а также регулярно обновлять операционную систему.

3.5 Шпионское ПО (Spyware)

Шпионское ПО – это тип вредоносного ПО, которое отслеживает действия пользователей без их ведома. Эти возможности шпионажа могут включать в себя мониторинг активности, сбор нажатий клавиш, сбор данных (информация об учетной записи, логины, финансовые данные) и многое другое. Шпионское ПО также часто имеет дополнительные возможности, от изменения настроек безопасности программного обеспечения или браузеров до вмешательства в сетевые соединения. Шпионское ПО распространяется, используя уязвимости программного обеспечения, связывая себя с лицензионным программным обеспечением или троянскими программами.

К данной категории вредоносных программ относятся:

- Клавиатурные шпионы — это программы для скрытной записи информации о нажимаемых пользователем клавишах

- Перехватчики паролей – это программы, предназначенные для несанкционированного сбора паролей и cookie-файлов на заражённом устройстве.

- Банковские трояны – программы использующие уязвимости браузера для создания поддельных сайтов банков, которыми пользуется пользователь, и дальнейшей кражи учётных данных, или подмены реквизитов переводов со счёта пользователя.

- Стилеры – программы, созданные для поиска в заражённой системе важной информации, такой как имена пользователей и пароли, номера кредитных карт, адреса электронной почты и т. д., а также отправки контактам пользователя фишинговых писем.

Основным способом защиты от шпионского ПО является установка антивируса.

Заключение

В наш век высоких технологий одной из актуальных проблем являются вредоносные программы. Технологии совершенствуются с огромной скоростью, что приводит к активному развитию вредоносного программного обеспечения. Поэтому необходимость защиты компьютера от воздействия вирусных программ и иного вредоносного ПО в настоящее время является одним из приоритетных направлений в сфере компьютерных технологий. Чтобы избежать проникновения вредоносного ПО на компьютер и вместе с тем всех его последствий, нужно правильно выбрать и установить антивирусную программу и соблюдать элементарные меры предосторожности.

Список литературы

1. Зверев В.С. Информатика: Учебное пособие для студентов вузов.

Астрахань, 2013.
2. Владимир Безмалый: статья «Распространенные типы вредоносного ПО» 2021

https://www.securitylab.ru/blog/personal/bezmaly/350756.php

3. Сергей Островский: статья «Компьютерные вирусы» ЗАО «ДиалогНаука»

http://www.k-press.ru/comp

4. Статьи Лаборатории Касперского, 2021 г. АО «Лаборатория Касперского»

https://www.kaspersky.ru/resource-center

5.Статья «Защита от вредоносных программ и спама»

http://yztm.ru/lekc2/l24/#post-1161-_Toc511786778