# Вредоносные программы

Выполнила: Сперанских В.В. ФЛ11-Б3

Оглавление

# Оглавление.

1) Что такое вредоносные программы?
2) Классификация вредоносных программ.
2.1) Классификация вредоносных программ.
3) Компьютерные вирусы.
3.1) Компьютерные вирусы.
3.2) Компьютерные вирусы.
4) Сетевые черви.
4.1) Сетевые черви.
5) Троянские программы.
5.1) Троянские программы.
6) Шпионское ПО.
7) Хакерские утилиты.
7.1) Хакерские утилиты.
7.2) Хакерские утилиты.
8) Основы работы антивирусных программ.

Выполнила: Сперанских В.В. ФЛ11-Б3

# 1) Что такое вредоносные программы?

Для начала следует разобраться с определением вредоносной программы. **Вредоносная программа** — 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.

Выполнила: Сперанских В.В. ФЛ11-Б3

Оглавление

# 2) Классификация вредоносных программ

Вредоносные программы классифицируют по способу проникновения, размножения и типу вредоносной нагрузки.

В соответствии со способами распространения и вредоносной нагрузки все вредоносные программы можно разделить на следующие типы: компьютерный вирус, червь, троян, шпионское ПО, хакерские утилиты.

Выполнила: Сперанских В.В. ФЛ11-Б3

Оглавление

# 2.1) Классификация вредоносных программ

Следует отметить, что компьютерным вирусом часто называют любую вредоносную программу. Это обусловлено тем, что первые известные вредоносные программы были именно компьютерными вирусами, и в течение последующих десятилетий число вирусов значительно превышало количество всех остальных вредоносных программ. Однако в последнее время наметились тенденции к появлению новых, невирусных технологий, которые используют вредоносные программы. При этом доля истинных вирусов в общем числе инцидентов с вредоносными программами за последние годы значительно сократилась.

Выполнила: Сперанских В.В. ФЛ11-Б3

Оглавление

# 3) Компьютерные вирусы

**Компьютерный вирус** – это программа, способная создавать свои дубликаты и внедрять их в компьютерные сети и/или файлы, системные области компьютера и прочие выполняемые объекты. При этом дубликаты сохраняют способность к дальнейшему распространению.

- Основная цель любого компьютерного вируса – это распространение на другие ресурсы компьютера и выполнение специальных действий при определенных событиях или действиях пользователя (например, 25-го числа каждого четного месяца или при перезагрузке компьютера). Специальные действия нередко оказываются вредоносными.

Выполнила: Сперанских В.В. ФЛ11-Б3

Оглавление

# 3.1) Компьютерные вирусы

Жизненный цикл любого компьютерного вируса можно разделить на четыре этапа:

1. проникновение на чужой компьютер;
2. активация;
3. поиск объектов для заражения;
4. подготовка и внедрение копий.

Путями проникновения вируса могут служить как мобильные носители, так и сетевые соединения – фактически все каналы, по которым можно скопировать файл. Однако, в отличие от червей, вирусы не используют сетевых ресурсов – заражение вирусом возможно, только если пользователь сам каким-либо образом его активировал, например, скопировал или получил по почте зараженный файл и сам его запустил или просто открыл.

Выполнила: Сперанских В.В. ФЛ11-Б3

Оглавление

# 3.2) Компьютерные вирусы

После проникновения следует активация вируса. Это может происходить разными путями, и в зависимости от выбранного метода вирусы делятся на такие виды:

- *загрузочные вирусы* – заражают загрузочные сектора жестких дисков и мобильных носителей;
- *файловые вирусы* – заражают файлы.

Дополнительным признаком отличия вирусов от других вредоносных программ служит их привязанность к операционной системе или программной оболочке, для которой каждый конкретный вирус был написан. Так, вирус для Microsoft Windows не будет работать и заражать файлы на компьютере с другой установленной операционной системой, например, Linux, UNIX или macOS.

Выполнила: Сперанских В.В. ФЛ11-Б3

Оглавление

# 4) Сетевые черви

В отличие от вирусов, сетевые черви – это вполне самостоятельные вредоносные программы. Главной их особенностью также является способность к саморазмножению, однако при этом они способны к самостоятельному распространению с использованием сетевых каналов.

В зависимости от способа проникновения в систему черви делятся на следующие типы:

- *сетевые черви* – используют для распространения локальные сети и Интернет;
- *почтовые черви* – распространяются с помощью почтовых программ;
- *IM-черви* – используют программы обмена сообщениями IM (Instant Messenger) в режиме реального времени;
- *P2P-черви* – распространяются при помощи пиринговых файлообменных сетей P2P (Peer-to-Peer – равный с равным).

Выполнила: Сперанских В.В. ФЛ11-Б3

Оглавление

# 4.1) Сетевые черви

После проникновения на компьютер червь должен активироваться – иными словами, запуститься. По методу активации все черви можно разделить на две большие группы: на тех, которые требуют активного участия пользователя, и тех, кто его не требует.

Отличительная особенность червей из первой группы – это использование обманных методов. Например, получатель инфицированного файла вводится в заблуждение текстом полученного письма и добровольно открывает вложение с почтовым червем, тем самым его активируя. Черви из второй группы используют ошибки в настройке или бреши в системе безопасности операционной системы. В последнее время наметилась тенденция к совмещению этих двух технологий – такие черви наиболее опасны и часто вызывают глобальные эпидемии.

Выполнила: Сперанских В.В. ФЛ11-Б3

Оглавление

# 5) Троянские программы

Троянская программа (программа класса «троянский конь») имеет только одно назначение – нанести ущерб целевому компьютеру путем выполнения не санкционированных пользователем действий: кражи, порчи или удаления конфиденциальных данных, нарушения работоспособности компьютера или использования его ресурсов в неблаговидных целях.

В отличие от вирусов и червей, трояны сами не размножаются.

Жизненный цикл троянов состоит всего из трех этапов:

1. проникновение в систему;
2. активация;
3. выполнение вредоносных действий.

Выполнила: Сперанских В.В. ФЛ11-Б3

Оглавление

# 5.1) Троянские программы

Некоторые трояны способны к самостоятельному преодолению систем защиты компьютерной системы с целью проникновения в нее. В этом случае обычно применяется маскировка, когда троян выдает себя за полезное приложение, которое пользователь самостоятельно копирует себе на диск (например, загружает из Интернета) и запускает. При этом программа действительно может быть полезна, однако наряду с основными функциями она может выполнять действия, свойственные трояну.

Однако в большинстве случаев трояны проникают на компьютеры вместе с вирусом либо червем – то есть такие трояны можно рассматривать как дополнительную вредоносную нагрузку, но не как самостоятельную программу.

После проникновения на компьютер трояну необходима активация, и здесь он похож на червя – либо требует активных действий от пользователя, либо через уязвимости в программном обеспечении самостоятельно заражает систему.

Однако в большинстве случаев трояны проникают на компьютеры вместе с вирусом либо червем – то есть такие трояны можно рассматривать как дополнительную вредоносную нагрузку, но не как самостоятельную программу.

После проникновения на компьютер трояну необходима активация, и здесь он похож на червя – либо требует активных действий от пользователя, либо через уязвимости в программном обеспечении самостоятельно заражает систему.

Выполнила: Сперанских В.В. ФЛ11-Б3

Оглавление

# 6) Шпионское ПО

*Шпионское ПО* – опасные для пользователя программы, предназначенные для слежения за системой и отсылки собранной информации третьей стороне – создателю или заказчику такой программы. Среди заказчиков шпионского ПО – спамеры, маркетинговые агентства, спам-агентства, преступные группировки, деятели промышленного шпионажа. Шпионские программы интересуются системными данными, типом браузера, посещаемыми веб- узлами, иногда и содержимым файлов на жестком диске компьютера-жертвы. Такие программы тайно закачиваются на компьютер вместе с каким-нибудь бесплатным софтом или при просмотре определенным образом сконструированных HTML-страниц и всплывающих рекламных окон и самоустанавливаются без информирования об этом пользователя. Побочные эффекты от присутствия шпионского ПО на компьютере – нестабильная работа браузера и замедление производительности системы;

Выполнила: Сперанских В.В. ФЛ11-Б3

Оглавление

# 7) Хакерские утилиты(rootkit)

Первоначально термин rootkit означал набор вредоносных приложений, скрывающих свое присутствие на компьютере и позволяющих хакеру делать свои дела незаметно. Слово root в названии явно указывает, что слово зародилось в мире Unix-компьютеров, но сегодня, когда мы говорим о руткитах, как правило речь ведется о Windows-компьютерах, и в понятие «руткит» включаются не только средства обеспечения скрытности, но и весь набор функций вредоносного приложения. Оно обычно прячется глубоко в недрах операционной системы и специально написано таким образом, чтобы избегать обнаружения антивирусами и другими средствами безопасности. Руткит может содержать различные вредоносные инструменты, такие как клавиатурный шпион, вор сохраненных паролей, сканер данных о банковских карточках, дистанционно управляемый бот для осуществления DDoS-атак, а также функции для отключения антивирусов.

Выполнила: Сперанских В.В. ФЛ11-Б3

Оглавление

# 7.1) Хакерские утилиты(rootkit)

Первично руткиты попадают на компьютер так же, как другие вредоносные приложения. Обычно используется уязвимость в браузере или плагине, также популярный способ заражения – через USB-флешки. Атакующие иногда даже оставляют зараженные флешки в общественных местах, где их может подобрать подходящая жертва. Затем руткит использует уязвимости ОС чтобы получить привилегированное положение в системе и устанавливает дополнительные компоненты, обеспечивающие удаленный доступ к компьютеру и другую вредоносную функциональность.

Выполнила: Сперанских В.В. ФЛ11-Б3

Оглавление

# 7.2) Хакерские утилиты(rootkit)

- Основная сложность борьбы с руткитами в том, что они активно противодействуют своему обнаружению, пряча свои файлы и ключи реестра от сканирующих программ, а также применяя другие методики. Существуют утилиты, специально созданные для поиска известных и неизвестных руткитов разными узкоспециальными методами, а также с помощью сигнатурного и поведенческого анализа.

Выполнила: Сперанских В.В. ФЛ11-Б3

Оглавление

# 8) Основы работы антивирусных программ

- Самыми эффективными средствами защиты от вирусов являются специальные программы, способные распознавать и обезвреживать вирусы в файлах, письмах и других объектах. Такие программы называются антивирусами, и для того, чтобы построить действительно надежную антивирусную защиту, использовать их нужно обязательно. В современных антивирусных продуктах используются два основных подхода к обнаружению вредоносных программ: сигнатурный и проективный/эвристический.
- *Сигнатурные методы* – точные методы обнаружения вирусов, основанные на сравнении файла с известными образцами вирусов.
- *Проактивные/эвристические методы* – приблизительные методы обнаружения, которые позволяют с определенной вероятностью предположить, что файл заражен.

Выполнила: Сперанских В.В. ФЛ11-Б3

Оглавление

# СПАСИБО ЗА ВНИМАНИЕ

Выполнила: Сперанских В.В. ФЛ11-Б3

Оглавление