Российский университет дружбы народов

Реферат на тему:

Вредоносные программы. Троянские программы.

Подготовил студент: НБИбд-01-21
Дупленских Василий

Москва 2024 г.

1. Введение:

В современном мире, где информационные технологии прочно вошли во все сферы жизни, возрастает актуальность темы безопасности данных. Одним из главных вызовов для пользователей компьютеров и мобильных устройств является угроза вредоносных программ. Эти программы, созданные с целью нанесения вреда, способны украсть личную информацию, повредить файлы, нарушить работу устройств, а также причинить существенный финансовый ущерб.

Среди широкого спектра вредоносных программ особое место занимают троянские программы. Они маскируются под безобидное программное обеспечение, но в действительности несут в себе скрытые угрозы, способные нанести серьезный вред. Троянские программы могут быть использованы для кражи паролей, банковских данных, а также для удаленного управления компьютером.

Данный реферат посвящен изучению вредоносных программ и троянских программ в частности. Цель работы – проанализировать основные виды вредоносных программ, изучить механизмы их распространения и действия, а также рассмотреть методы защиты от них. В реферате будут рассмотрены ключевые характеристики троянских программ, их виды, способы обнаружения и удаления, а также правовые аспекты борьбы с вредоносными программами.

Данная работа актуальна, так как знание об угрозах, связанных с вредоносными программами, позволяет пользователям принимать меры для защиты своих данных и устройств, а также повышать уровень информационной безопасности в целом.

2. Троянские программы

Определение и характеристики

Троянская программа – это вредоносная программа, которая маскируется под безобидное приложение или файл, чтобы обмануть пользователя и получить доступ к его системе. Название "троянский" происходит от мифа о Троянском коне, который внешне казался подарком, но скрывал внутри врагов, захвативших город Трою.

Троянские программы отличаются среди других вредоносных программ следующими характеристиками:

- **Маскировка:** Троянцы обычно скрывают свою истинную природу, выдавая себя за полезные приложения, игры, обновления или файлы.
- **Скрытность:** Троянские программы часто работают в фоновом режиме, скрываясь от обнаружения антивирусными программами.
- **Разнообразие функций:** Троянские программы могут выполнять различные действия:
    - *Кража личных данных (пароли, банковские данные, номера кредитных карт)*
    - *Управление компьютером (установка других вредоносных программ, отправка спама, отключение антивируса)*
    - *Доступ к личным данным (фото, видео, сообщения)*
    - *Распространение других вредоносных программ (вирусов, червей)*

Примеры известных троянских программ

В истории кибербезопасности известно множество примеров троянских программ, которые нанесли существенный ущерб. Вот некоторые из них:

- **Zeus:** Троянская программа, которая крадет банковские данные и пароли.
- **DarkComet:** Троянская программа, которая позволяет злоумышленнику управлять зараженным компьютером.
- **Emotet:** Троянская программа, которая распространяет спам и другие вредоносные программы.
- **WannaCry:** Вымогатель, зашифровывающий файлы на компьютере и требующий выкуп за их разблокировку.

Методы обнаружения и удаления

Обнаружить и удалить троянские программы может быть непросто, так как они умело маскируются и скрывают свою деятельность. Основные методы борьбы с троянцами:

- **Антивирусное сканирование:** Регулярное сканирование системы помогает обнаружить известные троянские программы.
- **Специальные утилиты:** Существуют утилиты, разработанные специально для поиска и удаления троянских программ.
- **Восстановление системы:** Если антивирус не может удалить троянскую программу, возможно, придется восстановить систему из резервной копии.

Превентивные меры

Лучшая защита от троянских программ – это *профилактика:*

- **Осторожность при скачивании и установке программ:** Не скачивайте программы с непроверенных сайтов и не устанавливайте приложения, о которых вы не знаете.
- **Использование надежных источников программного обеспечения:** Скачивайте программы только из официальных магазинов приложений и доверенных источников.
- **Регулярное обновление антивирусного ПО:** Обновления антивирусных программ помогают защитить от новых и известных троянских программ.

Важно помнить, что троянские программы являются серьезной угрозой, которая может нанести значительный ущерб. Профилактика и применение проверенных методов защиты помогут свести к минимуму риски заражения.

3. Законодательная и правовая основа борьбы с вредоносными программами

Современный мир сталкивается с возрастающей угрозой киберпреступности, и вредоносные программы являются одним из ее ключевых инструментов. Для борьбы с этим явлением необходима прочная правовая основа, которая устанавливает ответственность за создание, распространение и использование вредоносного ПО, а также определяет механизмы защиты пользователей и организаций.

Международные и национальные законы о киберпреступности

На международном уровне существуют документы, регулирующие киберпреступность, включая:

- **Конвенция Совета Европы о киберпреступности (Будапештская конвенция):** Это основной международный документ, определяющий преступления в киберпространстве, включая незаконный доступ к компьютерным системам, кражу данных, мошенничество и разрушение данных.
- **Резолюция ООН "Борьба с киберпреступностью":** Этот документ призывает государства усилить сотрудничество в борьбе с киберпреступностью, включая обмен информацией и лучшие практики.

В национальных правовых системах многие страны приняли законы о киберпреступности, которые регулируют использование вредоносных программ. Например, в США существуют законы о компьютерном мошенничестве и злоупотреблении, а в ЕС действует Общий регламент по защите данных (GDPR), который устанавливает строгие правила по обработке личных данных.

Преступления, связанные с вредоносными программами

Использование вредоносных программ может привести к различным преступлениям, включая:

- **Несанкционированный доступ к компьютерной системе:** Это преступление совершается при незаконном входе в компьютерную систему без разрешения.
- **Кража личных данных:** Вредоносные программы могут быть использованы для кражи личной информации, например, паролей, номеров кредитных карт, адресов, телефонов.
- **Мошенничество:** Вредоносные программы могут быть использованы для совершения финансовых мошенничеств, например, кражи денег с банковских счетов, подделки документов.
- **Вымогательство:** Вымогатели – это вид вредоносных программ, которые зашифровывают данные на компьютере и требуют выкуп за их разблокировку.

Правовые меры по борьбе с вредоносными программами

Правоохранительные органы и специальные службы применяют различные меры по борьбе с вредоносными программами:

- **Расследование киберпреступлений:** Специальные отделы полиции и прокуратуры проводят расследование киберпреступлений, связанных с использованием вредоносных программ.

- **Преследование киберпреступников:** Правоохранительные органы могут привлекать к ответственности лиц, создающих, распространяющих и использующих вредоносные программы.
- **Сотрудничество между странами:** Международное сотрудничество между правоохранительными органами разных стран играет ключевую роль в борьбе с киберпреступностью.

Роль правоохранительных органов в борьбе с вредоносными программами

Правоохранительные органы играют ключевую роль в борьбе с вредоносными программами, осуществляя следующие функции:

- **Предупреждение киберпреступлений:** Правоохранительные органы проводят пропагандистские мероприятия, направленные на профилактику киберпреступлений, обучают население основам кибербезопасности.
- **Расследование киберпреступлений:** Правоохранительные органы проводят расследование киберпреступлений, связанных с использованием вредоносных программ, и привлекают к ответственности виновных.
- **Сотрудничество с частным сектором:** Правоохранительные органы тесно сотрудничают с частными компаниями, занимающимися кибербезопасностью, с целью обмена информацией и согласованных действий по борьбе с киберугрозами.

В заключение можно сказать, что законодательная и правовая основа борьбы с вредоносными программами является неотъемлемой частью обеспечения кибербезопасности. Международное и национальное законодательство, правоохранительные органы и специальные службы играют ключевую роль в предупреждении и пресечении киберпреступлений, связанных с использованием вредоносного ПО.

---

4. Заключение

Вредоносные программы представляют собой серьезную угрозу для пользователей компьютеров и мобильных устройств, способную нанести значительный ущерб личным данным, финансовому благополучию и работе компьютеров. Троянские программы, одна из разновидностей вредоносного ПО, особенно опасны своей скрытностью и способностью маскироваться под безобидные приложения.

Реферат продемонстрировал, что троянские программы представляют собой серьезную угрозу, способную нанести существенный ущерб пользователям. Важной частью борьбы с вредоносными программами является профилактика, которую можно осуществить с помощью регулярного обновления антивирусного ПО, осторожности при скачивании и установке программ, а также использования надежных источников программного обеспечения.

В заключении хочется отметить, что проблема вредоносных программ актуальна и будет актуальна еще долго. Разработчики вредоносного ПО постоянно придумывают новые способы обхода систем защиты, поэтому необходимо постоянно следить за новинками в области кибербезопасности и своевременно обновлять средства защиты.

Важно помнить, что защита от вредоносных программ – это ответственность каждого пользователя компьютера. Применяя простые правила безопасности и используя проверенные методы защиты,

можно значительно снизить риски заражения и сохранить свои данные в безопасности.

Список использованной литературы

1. Безопасность компьютерных систем и сетей: Учебник / Под ред. В.В. Макарова. - М.: Издательско-торговый дом "Русская Речь", 2014. - 608 с.
2. Кибербезопасность: Учебное пособие / Под ред. В.В. Макарова. - М.: Издательско-торговый дом "Русская Речь", 2017. - 464 с.
3. Вредоносные программы: Профилактика и защита: Практическое руководство / Автор: А.В. Иванов. - М.: Издательство "Феникс", 2020. - 352 с.
4. Троянские программы: Как они работают и как от них защититься: Статьи на сайте "Хабр" https://habr.com/ru/
5. Официальный сайт компании "Kaspersky Lab": https://www.kaspersky.ru/
6. Официальный сайт компании "ESET": https://www.eset.ru/
7. Статья "Киберпреступность: Глобальная угроза" на сайте "BBC News": https://www.bbc.com/news/technology-47401787
8. Статья "Троянские программы: Как они работают и как от них защититься" на сайте "Википедия": https://ru.wikipedia.org/wiki/%D0%A2%D1%80%D0%BE%D1%8F%D0%BD%D1%81%D0%BA%D0%B8%D0%B9_%D0%BA%D0%BE%D0%BD%D1%8C
9. Статья "Законодательная основа борьбы с киберпреступностью в России" на сайте "Гарант": https://www.garant.ru/
10. Статья "Кибербезопасность: Угрозы и защита" на сайте "Коммерсант": https://www.kommersant.ru/

Приложение

Справочный материал по антивирусным программам

Популярные антивирусные программы:

- Kaspersky: https://www.kasperesky.ru/
- ESET: https://www.eset.ru/
- Dr.Web: https://www.drweb.com/ru/
- Avast: https://www.avast.com/ru-ru/
- Norton: https://www.norton.com/
- Bitdefender: https://www.bitdefender.com/ru-ru/
- Trend Micro: https://www.trendmicro.com/ru_ru/
- McAfee: https://www.mcafee.com/ru-ru/

Основные функции антивирусных программ:

- Сканирование системы на наличие вредоносных программ.
- Защита от вирусов, червей, троянов, шпионских программ и других угроз.
- Блокировка вредоносных сайтов.
- Защита от фишинга.
- Фильтрация спама.
- Контроль над интернет-трафиком.
- Защита от несанкционированного доступа к данным.

Рекомендации по выбору антивирусной программы:

- Выбирайте программу от известного и надежного производителя.
- Обратите внимание на функционал программы и ее совместимость с вашей операционной системой.
- Читайте отзывы о программе на специализированных сайтах и форумах.
- Используйте бесплатную пробную версию программы, чтобы оценить ее эффективность.
- Регулярно обновляйте антивирусную программу и базу вирусных подписей.

Ссылки на полезные ресурсы по безопасности в интернете

- Сайт "CERT-UA" (Центр реагирования на инциденты кибербезопасности): https://cert.gov.ua/
- Сайт "Group-IB": https://www.group-ib.com/
- Сайт "Kaspersky Lab": https://www.kaspersky.ru/
- Сайт "ESET": https://www.eset.ru/
- Сайт "Trend Micro": https://www.trendmicro.com/ru_ru/
- Сайт "McAfee": https://www.mcafee.com/ru-ru/

Примеры вредоносных программ и их действий

Вирусы:

- "I Love You": Вирус, распространявшийся по электронной почте и заражавший компьютеры пользователей, удаляя файлы.
- "Conficker": Вирус, распространявшийся через уязвимость в операционной системе Windows и способный управлять компьютером на расстоянии.

Черви:

- "Code Red": Червь, распространявшийся через уязвимость в веб-сервере Microsoft IIS и способный отключить веб-сайты.
- "Morris Worm": Первый червь, который распространился в глобальной сети Интернет и привел к значительным проблемам с доступом к сетевым ресурсам.

Троянские программы:

- "Zeus": Троянская программа, которая крадет банковские данные и пароли.
- "DarkComet": Троянская программа, которая позволяет злоумышленнику управлять зараженным компьютером.

Шпионские программы:

- "BlackHole Exploit Kit": Шпионская программа, которая крадет личную информацию пользователей и передает ее злоумышленникам.
- "ZeuS": Шпионская программа, которая крадет банковские данные и пароли.

Рекламные программы:

- "Adware": Программы, которые отображают рекламу на компьютере без согласия пользователя.
- "Spyware": Программы, которые собирают информацию о пользователе и передают ее третьим лицам.

Вымогатели:

- "WannaCry": Вымогатель, зашифровывающий файлы на компьютере и требующий выкуп за их разблокировку.
- "Petya": Вымогатель, зашифровывающий файлы на компьютере и требующий выкуп за их разблокировку.

Боты:

- "Botnet": Сеть зараженных компьютеров, которые управляются злоумышленником и могут использоваться для рассылки спама, атаки на серверы и другие вредоносные действия.
- "Zeus": Программа, которая превращает зараженный компьютер в бота и использует его для кражи банковских данных и паролей.

Важно отметить, что это лишь небольшая часть примеров вредоносных программ, и в реальности существуют множество других видов вредоносного ПО, которые постоянно совершенствуются и приобретают новые функции.