Вредоносные программы. Троянские программы.

Информационная безопасность

Махорин И. С.

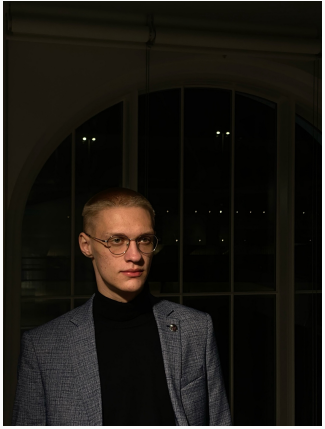
05 сентября 2024

Российский университет дружбы народов имени Патриса Лумумбы, Москва, Россия

Информация

Докладчик

- Махорин Иван Сергеевич
- Студент группы НПИбд-02-21
- Студ. билет 1032211221
- Российский университет дружбы народов имени Патриса Лумумбы



Вводная часть

Актуальность

Понятие «вредоносные программы» достаточно обширно и включает в себя множество видов специализированного ПО, среди которого выделяют: вирусы, троянских коней, логические бомбы, червей, шпионов и многое другое. Несмотря на бурное развитие антивирусов, вредоносные программы до сих пор представляют большую угрозу любой ИТ-инфраструктуре и ежегодно приносят большие убытки организациям различного размера.

Цели и задачи

- Произвести обзор вредоносных программ
- Проанализировать троянские программы
- Изучить методы защиты

Основная часть

Определение вредоносных программ

Вредоносное программное обеспечение (или просто вредоносная программа) — это программа, любая её часть или код, способные или целенаправленно написанные для нанесения вреда устройствам и данным, хранящимся на них.

Цели вредоносных программ

Цели вредоносных программ могут быть разными, например:

- получать несанкционированный доступ;
- использовать чужие вычислительные ресурсы;
- красть учётные данные;
- перехватывать управление;
- блокировать доступ;
- вымогать денежные средства.

Троянская программа

Троянская программа — это простейший вид вредоносных компьютерных программ.

Она маскируется под различное привлекательное для пользователя программное обеспечение, чтобы в процессе или после установки нанести вред компьютеру, использовать его ресурсы в своих целях или собрать необходимую информацию.

Троянская программа не является вирусом, поскольку лишена возможности распространяться самостоятельно.

Классификация троянских программ

- RAT (Remote Access / Administration Tool)
- Вымогатели
- Шифровальщики
- Загрузчики
- Дезактиваторы систем защиты
- Банкеры
- DDoS-трояны

Примеры известных троянских программ

Emotet впервые появился в 2014 году, но, как и Zeus, в настоящее время представляет собой модульную программу, которая чаще всего используется для доставки других форм вредоносных программ, например, Trickster и Ryuk.

Некоторые примеры последствий

- Во время пользования интернетом система сама переводит вас на страницы, которые вы не открывали.
- Нарушена работа антивируса. Он не включается вовсе или выдаёт ошибки при попытке использования.
- Панель инструментов Windows исчезла.
- Время от времени устройство выдаёт диалоговые окна, которые появляются независимо от ваших действий.
- Кнопка «Пуск» пропала или перестала работать.
- Не работает сочетание клавиш Ctrl + Alt + Del.
- Экран устройства самопроизвольно включается и выключается. Кроме того, его включение может сопровождаться появлением нетипичной заставки или «цветомузыки».

Меры для предотвращения проникновения

- Не открывайте электронные письма с незнакомых адресов.
- Регулярно обновляйте программы и приложения, которые установлены на ваших устройствах.
- Не пользуйтесь макросами в программах Word и Excel.
- Не переходите по незнакомым и сомнительным ссылкам.
- Загружайте любые программы только из проверенных источников.
- Зайдите в настройки и установите отображение всех расширений файлов.
- При посещении сайтов и сервисов, связанных с платёжными системами и владеющих конфиденциальными данными пользователя, используйте двухфакторную аутентификацию.
- Время от времени проверяйте систему на наличие вредоносных программ при помощи антивирусного ПО.
- Производите резервное копирование данных.

Вывод

В нашем докладе мы рассмотрели вредоносные программы, сосредоточив внимание на троянских программах, которые маскируются под обычные приложения для скрытого получения доступа к системе. Мы проанализировали их опасности и выявили, что эффективная защита включает использование антивирусного ПО, регулярное обновление программного обеспечения и повышение осведомленности пользователей о киберугрозах. Таким образом, комплексный подход к защите от вредоносных программ позволяет минимизировать риски и обеспечить безопасность данных.

Список литературы. Библиография

Список литературы. Библиография

[1] Информация о проблеме: https://studfile.net/preview/16426345/page:33/

[2] Информация о вредоносных программах: https://infobez.sakha.gov.ru/tpost/n0r2r08z01-vidi-vredonosnih-programm

[3] Информация о троянских программах: https://promopult.ru/library/Троянская_программа

[4] Информация о трояне Emotet: https://securitymedia.org/analytics/11-pechalno-izvestnykh-atak-vredonosnykh-programm-pervaya-i-samaya-strashnaya.html