Вредоносные программы. Троянские программы.

Информационная безопасность

Махорин Иван Сергеевич

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

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

2 Теоретическое введение

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 [1].

3 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 [2].

3.1 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.

3.2 Троянская программа

Троянская программа (англ. Trojan software; часто используют — троян, троянский конь, троянец) — простейший вид вредоносных компьютерных программ — маскируется под различное привлекательное для пользователя ПО, чтобы в про-

цессе или после установки нанести вред компьютеру, использовать его ресурсы в своих целях или собрать необходимую информацию [3].

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

3.3 Классификация троянских программ

Троянские программы можно классифицировать следующим образом:

- RAT (Remote Access / Administration Tool) — предназначены для шпионажа.
- Вымогатели — блокируют доступ к системе или данным, угрожают пользователю удалением файлов с компьютера или распространением личных данных жертвы в интернете и требуют заплатить выкуп.
- Шифровальщики — используют криптографию в качестве средства блокировки доступа.
- Загрузчики — предназначены для загрузки из интернета других программ или файлов.
- Дезактиваторы систем защиты — удаляют или останавливают антивирусы, сетевые экраны и другие средства обеспечения безопасности.
- Банкеры — специализируются на краже банковских данных.
- DDoS-трояны — используются хакерами для формирования ботнета с целью проведения атак типа «отказ в обслуживании».

3.4 Примеры известных троянских программ

Emotet - вредоносная программа, функциональность которой изменилась за годы, в течение которых она оставалась активной. Фактически, Emotet является ярким примером того, что известно как полиморфное вредоносное ПО, код которого немного меняется каждый раз при доступе к нему, чтобы избежать

распознавания программами безопасности конечных точек. Emotet - это троян, который в основном распространяется посредством фишинга [4].

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. Emotet настолько хорош в своем деле, что Арне Шенбом, глава Федерального ведомства по информационной безопасности Германии, называет его «королем вредоносных программ».

3.5 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.
- Изменился фон и общее цветовое решение W
- Кнопка «Пуск» пропала или перестала работать.
- Вы не можете войти в систему, потому что ваш пароль перестал быть актуальным.
- Не работает сочетание клавиш Ctrl + Alt + Del.
- Кнопки мыши перестали выполнять прежние функции.
- Экран устройства самопроизвольно включается и выключается. Кроме того, его включение может сопровождаться появлением нетипичной заставки или «цветомузыки».
- Принтер начал работать независимо от ваших команд.

3.6 Меры для предотвращения проникновения

- Не открывайте электронные письма с незнакомых адресов. Если в письме есть вложение, то подумайте, нужно ли вам его открывать. Такие документы и ссылки часто содержат в себе трояны.
- Регулярно обновляйте программы и приложения, которые установлены на ваших устройствах. Обновления призваны исправить уязвимые места в ПО и минимизировать риск проникновения вируса.
- Не пользуйтесь макросами в программах Word и Excel.
- Не переходите по незнакомым и сомнительным ссылкам. Они могут привести вас на поддельный сайт, который установит на ваше устройство вредоносное программное обеспечение в фоновом режиме.
- Загружайте любые программы только из проверенных источников. Особенно это касается мобильных приложений. Если нужная программа отсутствует в Google Play Store и Apple Store,то следует задуматься о её безопасности.
- Зайдите в настройки и установите отображение всех расширений файлов. Тогда вы сразу заметите, если какой-либо файл на самом деле является не тем, чем кажется. Например, изображение имеет расширение не jpg, а exe.
- При посещении сайтов и сервисов, связанных с платёжными системами и владеющих конфиденциальными данными пользователя, используйте двухфакторную аутентификацию. Это позволит обезопасить данные от злоумышленников и запретить доступ к вашему аккаунту даже в том случае, если им удастся завладеть паролем.
- Время от времени проверяйте систему на наличие вредоносных программ при помощи антивирусного ПО.
- Производите резервное копирование данных. Это касается как облачных сервисов, так и физических носителей информации.

4 Выводы

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.

5 Список литературы

[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