Виды вредоносного ПО

Сабина Жигальская
Специалист по комплексной защите информации

Skillbox

Цель урока

Узнать, какие виды вредоносов бывают.

Введение

Разновидностей достаточно много, рассмотрим каждую подробнее.

Ботнет

Ботнет — компьютерная сеть из устройств, заражённых вредоносной программой.

Ботом обычно называют устройство (компьютер, смартфон), находящееся под управлением скрытой программы, которая получает команды от своего хозяина через интернет.

Зомби = бот

Проникновение вредоносных программ может случиться при недостаточной бдительности пользователя: киберпреступники маскируют их под полезное ПО.

Вредоносные программы для организации бот-сетей самостоятельно запускаются на устройстве, защищаются от удаления.

Ботнет имеет огромные вычислительные ресурсы, приносит ощутимую прибыль киберпреступникам.

Объекты воздействия

Объектами воздействия ботнетов являются государственные структуры и коммерческие компании, обычные пользователи интернета.

Киберпреступники применяют боты для достижения целей разного содержания и величины.

Цели ботнетов

Бот-агенты создаются злоумышленниками, например, с целью воровства. Обычно взломщики похищают данные доступа к той или иной системе, желая получить денежную прибыль или какую-либо иную личную выгоду.

Зомби-сетями пользуются представители незаконного бизнеса, продвигая свой товар и услуги.

Эксплойты

Эксплойты — это хакерские утилиты, предназначенные для эксплуатации уязвимостей в программном обеспечении.

База данных эксплойтов хранится на сайте exploit-db.ru.

Бэкдор

Бэкдор — это программы для удалённого подключения к компьютеру и управления им.

Бэкдоры выполняют две основные функции: оперативное получение доступа к данным и удалённое управление компьютером.

Вирусы

Вирусом принято называть программу, которая внедряет свой код в другие приложения («заражает» их), так что при каждом запуске инфицированного объекта этот код исполняется.

Компьютерные вирусы могут внедряться в код других приложений и воспроизводиться, выполняя копирование самих себя.

Руткит

Руткиты — средства скрытия вредоносной деятельности (например, другие приложения не смогут обнаружить файлы, принадлежащие нежелательному ПО).

Трояны

Троянские кони» («трояны») — широкий класс вредоносных объектов разнообразного назначения, которые обычно не имеют собственного механизма распространения (т. е. не могут заражать файлы или размножать свои копии через сеть).

Один из самых распространённых видов троянов — это вымогатели — разновидность вредоносных объектов, которые блокируют доступ к системе или данным, угрожают пользователю удалением файлов с компьютера или распространением личных данных жертвы в интернете и требуют заплатить выкуп, чтобы избежать таких негативных последствий.

Выводы урока

- Существует немало видов вредоносов, и у них разные цели. Кто-то балуется, а кто-то жаждет наживы
- Умение определять вид вредоноса очень важно для системного администратора

Выводы модуля

- Мы рассмотрели более подробно, как устроены модели управления доступом и как они используются
- Далее мы разобрали классификацию вредоносов. Их немало, и у них разные цели
- Системный администратор должен уметь определять вид вредоноса по нанесённому вреду