КИБЕРПРЕСТУПНОСТЬ

Подготовил Илья Бочаров

ОГЛАВЛЕНИЕ

1.КИБЕРБЕЗОПАСНОСТЬ

- Кибербезопасность (ее иногда называют компьютерной безопасностью) – это совокупность методов и практик защиты от атак злоумышленников для компьютеров, серверов, мобильных устройств, электронных систем, сетей и данных. Кибербезопасность находит применение в самых разных областях, от бизнес-сферы до мобильных технологий. В этом направлении можно выделить несколько основных категорий.

1.1 БЕЗОПАСНОСТЬ СЕТЕЙ

- Действия по защите компьютерных сетей от различных угроз, например целевых атак или вредоносных программ.

1.2 БЕЗОПАСНОСТЬ ПРИЛОЖЕНИЙ

- Защита устройств от угроз, которые преступники могут спрятать в программах. Зараженное приложение может открыть злоумышленнику доступ к данным, которые оно должно защищать. Безопасность приложения обеспечивается еще на стадии разработки, задолго до его появления в открытых источниках.

1.3 БЕЗОПАСНОСТЬ ИНФОРМАЦИИ

- Обеспечение целостности и приватности данных как во время хранения, так и при передаче.

1.4 АВАРИЙНОЕ ВОССТАНОВЛЕНИЕ И НЕПРЕРЫВНОСТЬ БИЗНЕСА

- Реагирование на инцидент безопасности (действия злоумышленников) и любое другое событие, которое может нарушить работу систем или привести к потере данных. Аварийное восстановление – набор правил, описывающих то, как организация будет бороться с последствиями атаки и восстанавливать рабочие процессы. Непрерывность бизнеса – план действий на случай, если организация теряет доступ к определенным ресурсам из-за атаки злоумышленников.

1.5 ПОВЫШЕНИЕ ОСВЕДОМЛЕННОСТИ

- Обучение пользователей. Это направление помогает снизить влияние самого непредсказуемого фактора в области кибербезопасности – человеческого. Даже самая защищенная система может подвергнуться атаке из-за чьей-то ошибки или незнания. Поэтому каждая организация должна проводить тренинги для сотрудников и рассказывать им о главных правилах: например, что не нужно открывать подозрительные вложения в электронной почте или подключать сомнительные USB-устройства

2. КИБЕРУГРОЗЫ

- **Киберпреступление**– действия, организованные одним или несколькими злоумышленниками с целью атаковать систему, чтобы нарушить ее работу или извлечь финансовую выгоду.
- **Кибератака** – действия, нацеленные на сбор информации, в основном политического характера.
- **Кибертерроризм** – действия, направленные на дестабилизацию электронных систем с целью вызвать страх или панику.

2.1 ВРЕДОНОСНОЕ ПО (ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ)

- **Вредоносное ПО** — это назойливые или опасные программы, предназначенные для тайного доступа к устройству без ведома его владельца.

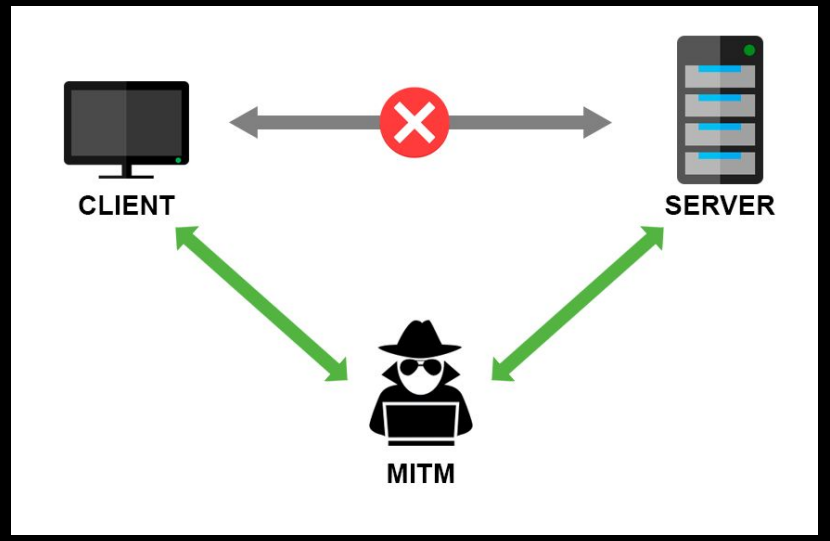
- Я хочу выделить несколько типов вредоносного ПО:
  1. **Вирусы**
  2. **Троянцы**
  3. **Шпионское ПО**
  4. **Программы-вымогатели**
  5. **Рекламное ПО**

2.2 ФИШИНГ

- Атаки, цель которых – обманом заполучить конфиденциальную информацию пользователя (например, данные банковских карт или пароли). Часто в ходе таких атак преступники отправляют жертвам электронные письма, представляясь офиц

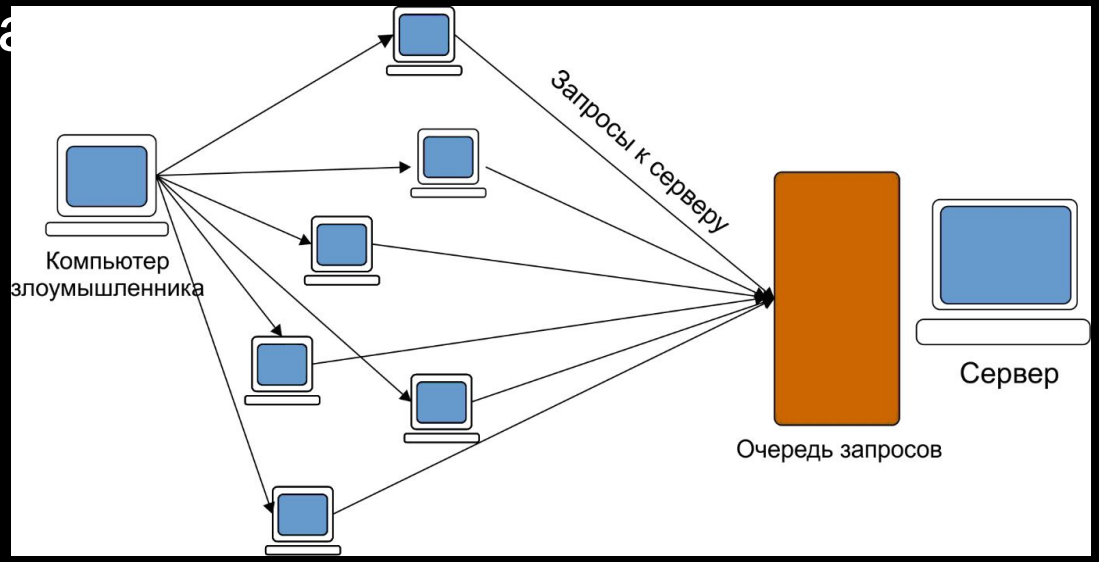
2.3 АТАКИ MAN-IN-THE-MIDDLE («ЧЕЛОВЕК ПОСЕРЕДИНЕ»)

- Это атака, в ходе которой киберпреступник перехватывает данные во время их передачи – он как бы становится промежуточным звеном в цепи, и жертвы об этом даже не подозревают. Вы можете подвергнуться такой атаке, если, например, подключитесь к незащищенной сети Wi-Fi.



2. 4 DOS-АТАКИ (АТАКИ ТИПА «ОТКАЗ В ОБСЛУЖИВАНИИ»)

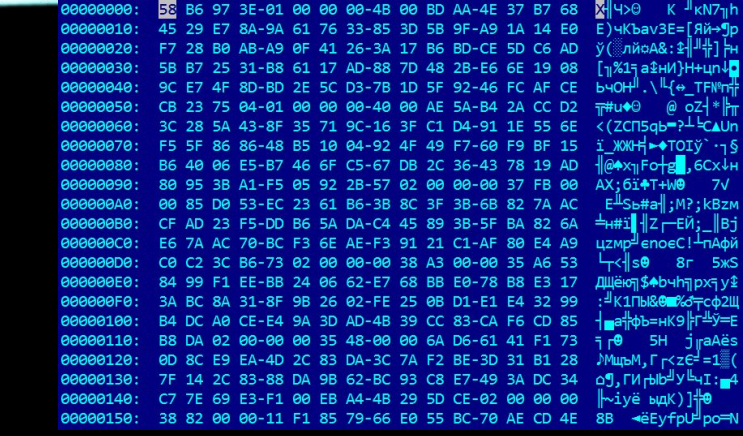
- Киберпреступники создают избыточную нагрузку на сети и серверы объекта атаки, из-за чего система прекращает нормально работать и ею становится невозможно пользоваться. Так злоумышленники, например, могут повредить важные компоненты инфраструктуры и саботировать деятельность орга



3. НОВЕЙШИЕ КИБЕРУГРОЗЫ

- С какими из новейших киберугроз сталкиваются пользователи и организации? Рассмотрим некоторые из тех, что попали в отчеты правительств Великобритании, США и Австралии.

3.1 ТРОЯНЕЦ DRIDEX



- В декабре 2019 года Министерство юстиции США обвинило лидера группы киберпреступников в участии в атаке с использованием Dridex. Эта кампания затронула общественные, правительственные и деловые структуры по всему миру.
- Dridex – банковский троянец* с широким набором возможностей, который появился в 2014 году. Он проникает на компьютеры жертв с помощью фишинговых писем и вредоносных программ. Dridex может красть пароли, данные банковских карт и личную информацию пользователей, которые затем используют мошенники. Размер причиненного им финансового ущерба исчисляется сотнями миллионов.
- Чтобы защититься, Национальный центр кибербезопасности Великобритании рекомендует устанавливать на устройства последние обновления безопасности и антивирусное ПО свежих версий, а также регулярно выполнять резервное копирование файлов.

*троянец **это тип вредоносных программ, маскирующихся под легитимное ПО. Он часто используется киберпреступниками для кражи личных данных, слежения за пользователями и получения несанкционированного доступа к системам.**

3.2 ВИРУС PETYA

- Вирус Petya известен также под другими названиями: Petya.A, PetrWrap, NotPetya, ExPetr. Попадая в компьютер, он скачивает из интернета шифровальщик и пытается поразить часть жесткого диска с данными, необходимыми для загрузки компьютера. Если ему это удается, то система выдает Blue Screen of Death («синий экран смерти»). После перезагрузки выходит сообщение о проверке жесткого диска с просьбой не отключать питание. Таким образом, вирус-шифровальщик выдает себя за системную программу по проверке диска, шифруя в это время файлы с определенными расширениями. В конце процесса появляется сообщение о блокировке компьютера и информация о том, как получить цифровой ключ
ифровки данных. Вирус Petya требует выкупа, как правило,
нах.

4. КАК НЕ СТАТЬ ЖЕРТВОЙ КИБЕРПРЕСТУПЛЕНИЙ

- - храните номер карточки и ПИН–коды в тайне;
- - не используйте один пароль для всех интернет-ресурсов;
- - к своей основной карте в Вашем банке выпустите дополнительную, которой будете расплачиваться в интернете. Туда легко можно будет переводить небольшие суммы денег, и в случае компрометации данных достаточно просто заблокировать ее;
- - регулярно проверяйте состояние своих банковских счетов, чтобы убедиться в отсутствии «лишних» и странных операций;
- - поставьте лимит на сумму списаний или перевода в личном кабинете банка;
- - не перечисляйте деньги на электронные кошельки и счета мобильных телефонов при оплате покупок, если Вы не убедились в благонадежности лица/организации, которым предназначаются Ваши средства;
- - не переводите денежные средства на счета незнакомых лиц;
- - не перезванивайте и не направляйте ответные SMS, если Вам поступило сообщение о блокировании банковской карты. Свяжитесь с банком, обслуживающим Вашу карту;
- - будьте осмотрительны в отношении писем с вложенными картинками, поскольку файлы могут содержать вирусы. Открывайте вложения только от известных Вам отправителей. И всегда проверяйте вложения на наличие вирусов, если это возможно;
- - не переходите необдуманно по ссылкам, содержащимся в спам-рассылках. Удостоверьтесь в правильности ссылки, прежде чем переходить по ней из электронного письма;
- - не заполняйте полученные по электронной почте формы и анкеты. Личные данные безопасно вводить только на защищенных сайтах;
- - насторожитесь, если от Вас требуют немедленных действий или представляется чрезвычайная ситуация. Это тоже может быть мошенничеством. Преступники вызывают у Вас ощущение тревоги, чтобы заставить Вас действовать быстро и неосмотрительно;
- - не размещайте в открытом доступе и не передавайте информацию личного характера.