**Что такое ботнет?**

Botnet — это сеть из зараженных вредоносным программным обеспечением (ПО) устройств, которые управляются киберпреступниками. Слово "ботнет" образовано от английских слов robot (робот) и network (сеть). Зараженные устройства, называемые **ботами** или **зомби**, могут включать компьютеры, ноутбуки, смартфоны и даже IoT-устройства. Пользователи этих устройств часто не подозревают о том, что их машины участвуют в ботнете.

**Технология Botnet**

Существует две основные модели организации ботнетов:

1. **Клиент-серверная модель**: В этой модели боты подключаются к одному или нескольким управляющим серверам. Серверы отправляют команды ботам, которые выполняют указания и отчитываются о результатах. Недостатком этой модели является уязвимость серверов, которые могут быть обнаружены и отключены специалистами по безопасности.
2. **Децентрализованная (P2P) модель**: В этом случае боты обмениваются данными друг с другом без центрального сервера. Каждый бот может выполнять функции как клиента, так и сервера. Эта модель более устойчива к атакам, так как нет единой точки отказа, но управление становится сложнее.

**Процесс заражения**

Для создания ботнета злоумышленники используют различные методы заражения устройств:

* Рассылка электронных писем со зловредными вложениями.
* Эксплуатация уязвимостей в программном обеспечении.
* Использование вирусов или червей для автоматического распространения.

После заражения устройства становятся частью ботнета и могут выполнять команды злоумышленника.

## **Примеры ботнет атак**

Ботнеты используются для различных киберпреступлений, включая:

* **DDoS-атаки**: Массовые атаки на серверы с целью их перегрузки и отключения.
* **Рассылка спама**: Автоматизированная рассылка нежелательных сообщений.
* **Кража данных**: Сбор конфиденциальной информации с зараженных устройств.
* **Майнинг криптовалюты**: Использование ресурсов зараженных машин для добычи криптовалюты.

## Заключение

Ботнеты представляют собой серьезную угрозу в современном киберпространстве. Они могут наносить значительный ущерб как отдельным пользователям, так и организациям. Для борьбы с ботнетами необходимы комплексные меры по их обнаружению и уничтожению, а также повышение уровня киберграмотности среди пользователей.