EDGE ЦЕНТР

АРПП Отечественный софт

Искусственный интеллект и кибербезопасность: Новейшие подходы к защите от DDoS атак, ботов и хактивистов

Артём Избаенков

Директор по развитию направления кибербезопасности

Член правления АРСИБ

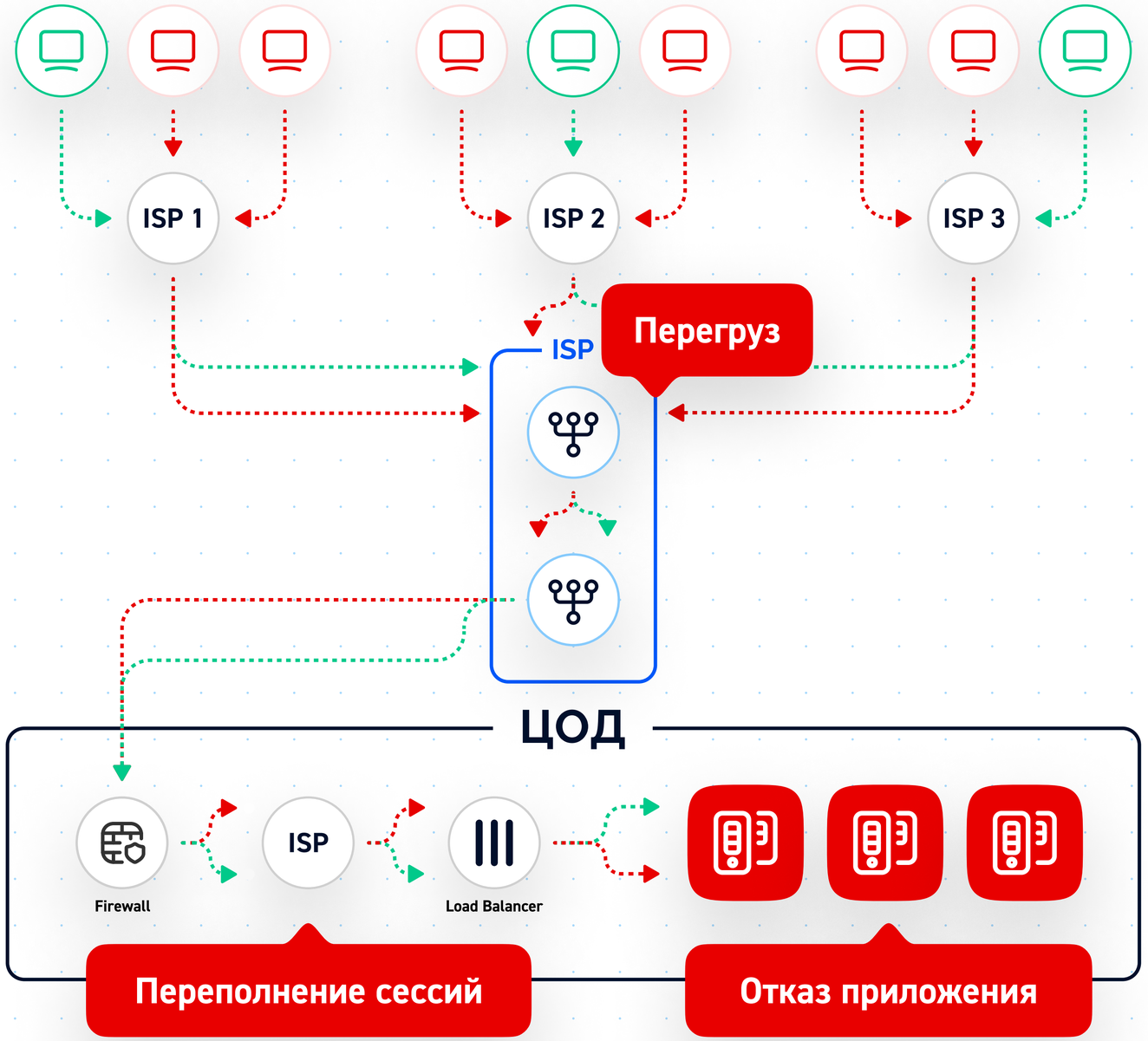
Член ISDEF

Член РОЦИТ

Сложность современных DDoS-атак

Сегодня DDoS-атаки можно разделить на 3 типа:

1. Перегрузку канала
2. Переполнений таблиц сессий
3. Отказ сервиса (приложения)



EDGE ЦЕНТР

Самые распространённые бот-атаки

DoS- и DDoS-атаки

Боты генерируют огромное количество запросов, чтобы сделать ресурсы недоступными.

Брутфорс

Боты взламывают аккаунты с помощью автоматического перебора паролей.

Скрейпинг

Боты собирают данные с сайтов и могут, например, передать их конкурентам или использовать для спам-рассылок и т.п.

Поиск уязвимостей

С помощью ботов злоумышленники ищут уязвимости приложений и эксплуатируют zero-day уязвимости.

Рекламный фрод

Боты могут кликать на платную рекламу. В итоге компания платит за трафик, который не конвертируется в покупки, ухудшаются позиции сайта в поисковой выдаче.

Скальперские покупки

Злоумышленники автоматически скупают ограниченный товар, чтобы перепродать его дороже.

Кардинг

Боты могут использовать украденные данные карт, чтобы покупать товары без участия владельцев карт.

Искажённая аналитика

Бот-трафик искажает реальную картину поведения пользователей. Компании не получают достоверных данных и не могут оптимизировать конверсии.

Исчерпание товаров (Denial of Inventory)

Товары: например, заполнить корзины или забронировать весь товар. Реальные пользователи не смогут его купить, но товар так и не будет продан.

Глоссарий

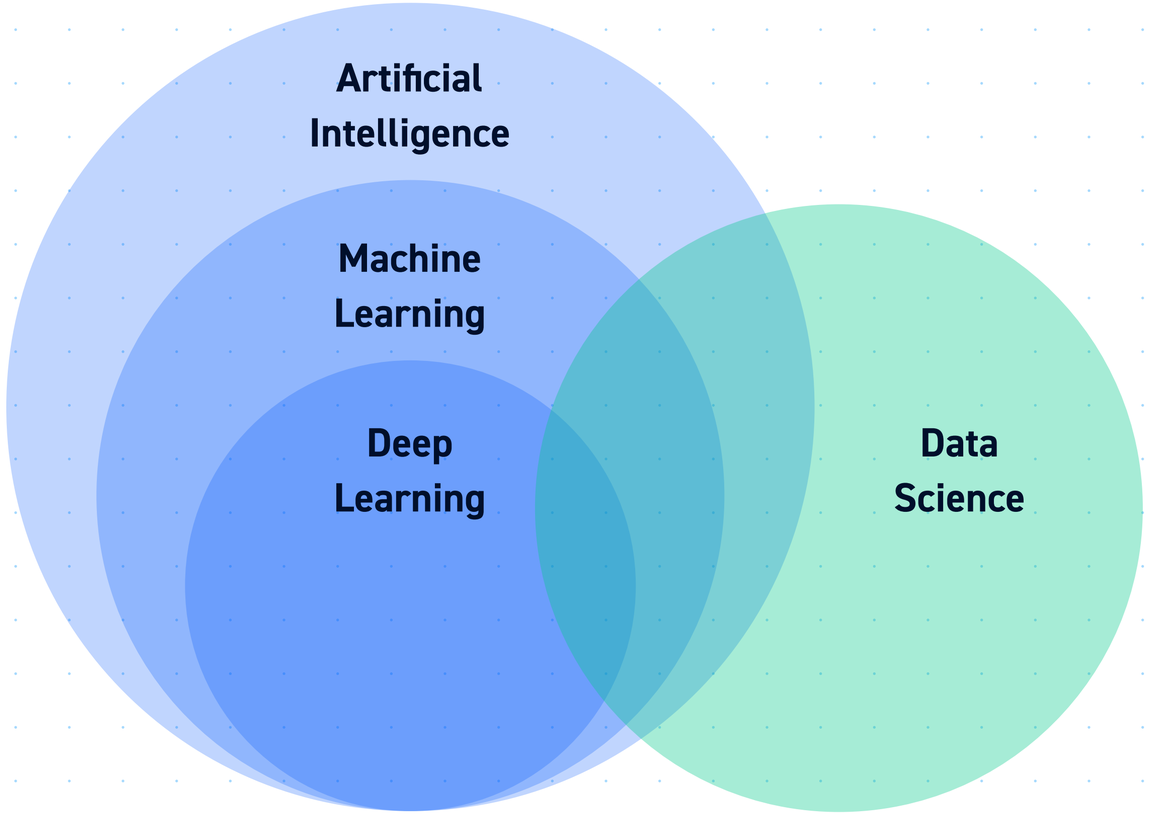
Машинное обучение (Machine learning)

Создание и использование инструментов для извлечения закономерностей из данных путем использования статистических и метрических методов на основе подготовленных датасетов.

Глубокое обучение (Deep learning)

Создание и использование нейронных сетей со специальными слоями, которые позволяют работать с данными сложной структуры.

Например, для работы с изображениями используют сверточные слои. Для текста — рекуррентные слои и эмбеддинги.



Data Science

Блокировка ботов

Алгоритм на основе параметров клиентского соединения определяет, действительно ли на сайт заходит человек с помощью браузера.

Если же это автоматизированный запрос бота — сессия блокируется.

Определение вектора DDoS-атаки

У любой DDoS-атаки есть особенности, выделяющие её среди множества других запросов.

Алгоритм находит совокупность параметров, по которым можно заблокировать атаку и не затронуть легитимных пользователей.

EdgeVector

Методы анализа признаков (Feature Analysis)

Этот подход заключается в выделении и анализе определенных признаков из сетевого трафика, которые могут указывать на DDoS-атаку.

Некоторые из таких признаков могут включать в себя **интенсивность трафика, количество пакетов в секунду, распределение источников трафика, сетевую пропускную способность** и другие.

Важно отметить

Для эффективного обнаружения векторов DDoS-атак необходимо иметь хорошо подготовленные и разнообразные обучающие данные, которые содержат как нормальный сетевой трафик, так и различные виды DDoS-атак. Также требуется постоянное обновление и адаптация моделей машинного обучения для борьбы с новыми и развивающимися видами DDoS-атак.

BotGate

Классификация на основе признаков (Feature-Based Classification)

В этом подходе используются алгоритмы машинного обучения для классификации запросов или поведения пользователей на основе определенных признаков, которые могут указывать на использование автоматизированных ботов.

Некоторые из таких признаков могут включать в себя:

- частоту запросов;
- скорость выполнения действий;
- типы запросов;
- пользовательские User Agent и другие.

Модели машинного обучения, такие как метод опорных векторов (SVM), случайный лес (Random Forest), градиентный бустинг (Gradient Boosting) в нашем случае справились отлично.

BotGate

Обнаружение необычного трафика (Unusual Traffic Detection)

В этом подходе используются алгоритмы машинного обучения для обнаружения необычного трафика на сайте, который может указывать на присутствие автоматизированных ботов. Можно использовать методы обнаружения аномалий, которые будут искать аномальные образцы трафика, такие как высокая интенсивность запросов с одного IP-адреса или необычные комбинации запросов.

Модели машинного обучения, такие как методы кластеризации, нейронные сети или методы градиентного бустинга, могут быть применены для обнаружения таких аномалий.

BotGate

Анализ временных рядов (Time Series Analysis)

Данные о поведении пользователей на сайте могут быть представлены в виде временных рядов, где каждая точка данных соответствует определенному временному интервалу.

Методы анализа временных рядов, такие как авторегрессионные интегрированные скользящие средние (ARIMA), рекуррентные нейронные сети (RNN) и сверточные нейронные сети (CNN), могут быть использованы для обнаружения аномалий во временных рядах, связанных с активностью ботов.

EDGE ЦЕНТР

edgecenter.ru

8 800 775 08 54