«Когда трафик становится разумным: как отличить атакующего ИИ от живого пользователя»

В эпоху стремительной цифровизации бизнеса вопросы кибербезопасности выходят на первый план, особенно в свете активности хактивистов.

Артем Избаенков

Директор продукта Solar Space ГК "Солар"

Консультант ООН по информационной безопасности

Член правления АРСИБ

Член РОЦИТ

Проблема хакерских атак нового уровня

Что такое боты?

От скриптов к “разумному” трафику

Тренды:

- 51 % всего интернет-трафика в 2024 году генерируется ботами .

Боты — это автоматические программы, которые имитируют действия пользователя в сети.

Эволюция:

- Раньше: простые скрипты (клики, парсинг).
- Сегодня: ИИ-агенты, которые умеют «думать» и копировать человеческое поведение.

Проблема: становится всё сложнее отличить человека от атакующего ИИ.

Разумный трафик — новая угроза

Когда трафик становится разумным

- ИИ-агенты кликают, прокручивают, пишут комментарии.
- Используют «человеческие» паузы и имитацию движений.
- Могут вести сложные цепочки действий.
- Размывается граница между ботом и человеком.

Вектора атак ИИ-ботов

Как атакует разумный трафик

DoS- и DDoS-атаки

ИИ-боты генерируют огромный поток запросов, распределяя нагрузку по тысячам узлов и подстраивая трафик так, чтобы он выглядел «естественно»

Брутфорс

Боты автоматически перебирают комбинации паролей, используя ML для приоритезации самых вероятных (например, по утечкам и частоте использования).

Скрейпинг

ИИ-боты массово собирают данные с сайтов: тексты, цены, изображения. Эти данные могут использоваться конкурентами.

Поиск уязвимостей

Боты сканируют веб-приложения и API на наличие ошибок конфигурации и «zero-day» уязвимостей. ИИ помогает автоматизировать распознавание слабых мест и эксплуатацию.

Атака на API

Шквал «умных» запросов к API, маскирующихся под легитимные, приводит к перегрузке сервисов и сбоям в работе бизнес-логики.

Рекламный фрод

ИИ-боты кликают на платную рекламу и создают «мусорный трафик». Бизнес тратит бюджет, не получая реальных клиентов.

Спам-атака (Spam Attack)

Генерация миллионов сообщений в формы обратной связи, чаты и e-mail. Цель — перегрузить каналы поддержки и снизить качество обслуживания.

Искаженная аналитика

Бот-трафик фальсифицирует данные: завышает или занижает показатели посещаемости, конверсии, CTR. Маркетинговые решения принимаются на недостоверных данных.

SEO-атака (Search Engine Manipulation)

ИИ-боты могут массово создавать ссылки, комментарии или кликать по конкурентам. Это ухудшает рейтинг вашего сайта и продвигает чужие ресурсы.

Почему старые методы защиты не работают

Классические механизмы больше не спасают

Капчи взламываются ИИ → точность выше, чем у человека.

Сигнатуры бесполезны → каждый бот уникален.

IP и User-Agent легко подменяются.

Нужен новый уровень защиты

Новый подход: ИИ против ИИ

Как защититься от разумного трафика

AntiBots ML

на страже вашего веб-приложения

Works Like Magic

Обучение Machine Learning алгоритмов на BigData позволила нам обучить феноминальную систему, которая легла в основу нашего патента и инноваций

BigData

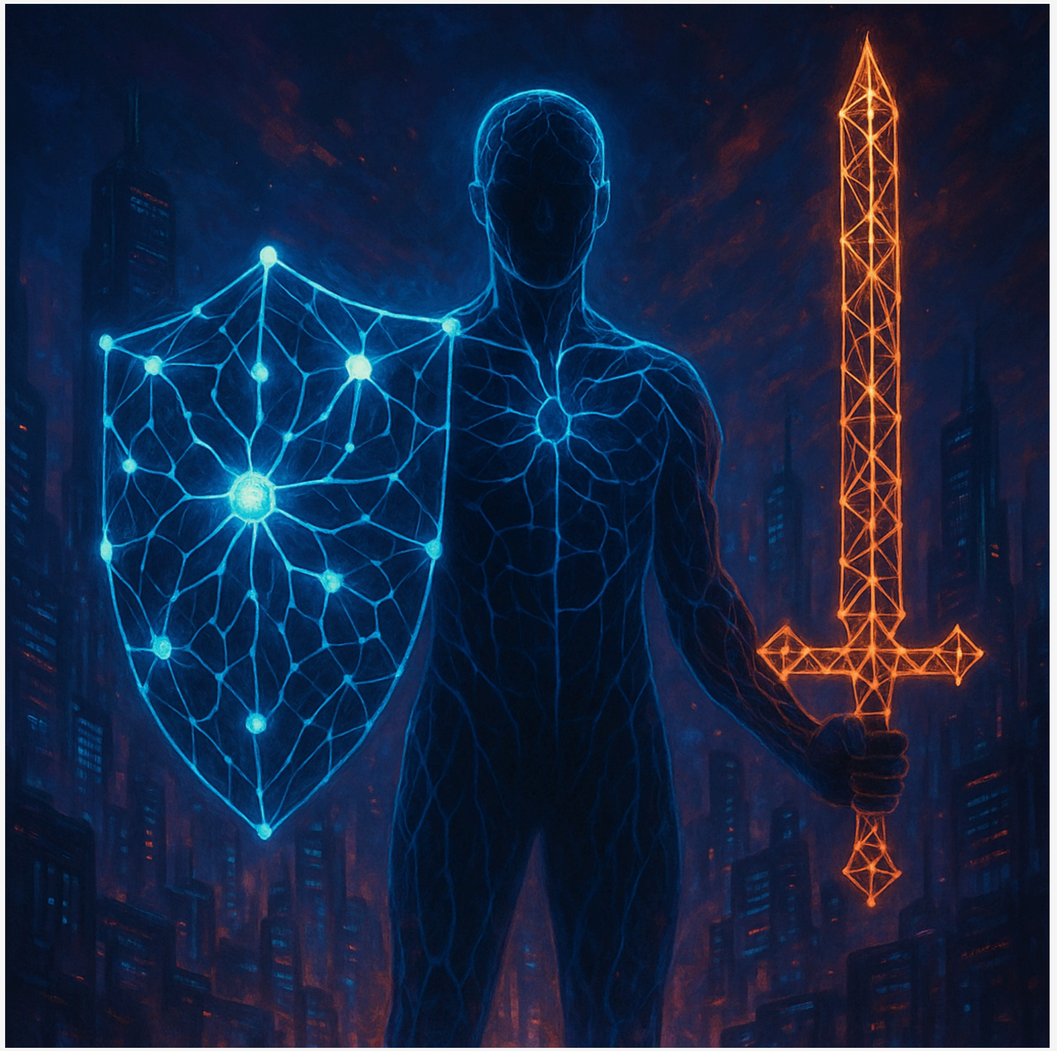
Более 1 млн DDoS атак, качественно выверенные датасеты группой экспертов и аналитиков на рынке ИБ

Постоянно развивается

Система разработана с учетом возможности дообучения и обучения на своих ошибках. Контроллером выступает CAPTCHA

Будущее: симбиоз человека и ИИ

- Разумный трафик — это уже реальность, а не теория.
- Атакующий ИИ становится всё изощрённее → защита должна быть не слабее.
- Только симбиоз: ИИ выявляет, человек верифицирует.
- Мы уже строим практику «ИИ против ИИ».



“Многие говорят, что Мир изменить нельзя, а мы с командой его меняем”

Артем Избаенков

Директор продукта Solar Space ГК “Солар”

Консультант ООН по информационной безопасности

Член правления АРСИБ

Член РОЦИТ