5 кибератак, которые сложно обнаружить без средств ИИ

Введение. ИИ как необходимое условие для кибербезопасности

Главное, что беспокоит ИТ-специалистов и специалистов по безопасности, — это растущая изощренность угроз, которым подвергаются корпоративные системы безопасности и вычислительные среды.

Злоумышленники научились скрывать и автоматизировать атаки, а их методы настолько разнообразны, что даже повторные атаки никогда не бывают одинаковыми. ИТ-среды становятся все более сложными: по прогнозам LogicMonitor, к концу 2020 г. 83% всех рабочих нагрузок ИТ будет выполняться в облаке. Все больше рабочих нагрузок приходится на долю пользователей, работающих удаленно. Интернет вещей ежегодно пополняется миллиардами устройств. Таким образом, контролировать облако становится намного сложнее, чем периметр традиционных локальных сред. В облаке нет четких границ, которые можно было бы защитить. Кроме того, ситуацию усложняет большой дефицит квалифицированных специалистов по кибербезопасности.

Из всего вышеперечисленного можно сделать вывод, что ИИ — не просто самое эффективное, а единственно возможное решение. Преимущество средств ИИ заключается в том, что они позволяют управлять большими объемами трафика без привлечения дополнительных специалистов.

Различные типы ИИ

Существует распространенное мнение, что все средства ИИ одинаковы. Однако это не так. Важно понимать, какими возможностями обладает ИИ и что подразумевают под этим поставщики, использующие ИИ.

Искусственный интеллект — это обширное научное направление. Оно включает в себя экспертные системы, то есть обучаемые вычислительные системы, способные принимать решения в определенной предметной области. ИИ также включает в себя машинное обучение. **Неконтролируемое машинное обучение** подразумевает самостоятельный поиск отклонений или изменений в поведении или активности.

Другой тип ИИ, **контролируемое машинное обучение**, предназначен для поиска по критериям, заданным в процессе обучения. Во многих случаях этот процесс обучения автоматизируется и используется в системах, определяющих, нужно ли выводить какие-либо данные.

Глубинное обучение — это квинтэссенция всех возможностей ИИ. В качестве примера можно привести программу распознавания символов, основанную на технологии глубинного обучения: сначала задействуется модуль ИИ для определения границ символов, а затем — модуль ИИ, определяющий язык по результатам первоначального анализа формы букв.

Теперь, когда у вас есть общее представление о типах ИИ, перейдем к рассмотрению различных комбинаций этих типов, позволяющих эффективно обнаруживать даже самые трудноуловимые атаки.

5 кибератак, которые сложно обнаружить без средств ИИ

Атака №1. Emotet

Emotet — это модульная троянская программа для атак на банковские системы, которая используется в течение многих лет и получает всё большее распространение. **По данным US-CERT**, «всего одна атака с использованием Emotet может привести к убыткам в миллионы долларов».

У программы Emotet есть интересная особенность: она «одноразовая», то есть предназначена для однократных атак. Кроме того, она полиморфна и каждый раз меняет форму. В эту программу также встроен механизм обфускации, который значительно затрудняет ее обнаружение.

Решение VMware NSX Advanced Threat Analyzer впервые обнаружило Emotet еще в 2015 г., но сейчас, спустя несколько лет, такие атаки происходят все чаще. Это объясняется полиморфизмом программы, из-за которого ее невозможно обнаружить с помощью стандартных моделей распознавания сигнатур.

Индийская притча о шести слепых

Чтобы объяснить, как NSX Advanced Threat Analyzer обнаруживает Emotet с помощью средств ИИ, вспомним древнюю индийскую притчу о шести слепых, которым впервые в жизни встретился слон. Слепые окружили слона и стали его ощупывать, каждый со своей стороны.

Один нащупал хвост и был убежден, что слон похож на веревку. Другой взялся за бивень и стал утверждать, что слон похож на копье. Третий обхватил ногу и заявил, что слон похож на дерево.

Все слепые были неправы, потому что никто из них не мог ощупать слона целиком. Они не видели полную картину. Кроме того, слепые не взаимодействовали друг с другом и не могли составить единое впечатление о слоне. В случае с Emotet то же самое происходило с антивирусными программами, которые не могли точно определить, что они обнаружили.

NSX Advanced Threat Analyzer обнаруживает Emotet с помощью контролируемого машинного обучения и комбинации экспертных систем. Контролируемое машинное обучение можно образно представить в виде людей, ощупывающих различные части тела слона и собирающих различные данные. Модуль ИИ принимает итоговое решение на основе данных о слоне, полученных в процессе контролируемого машинного обучения.

Именно так VMware NSX Network Detection and Response обнаруживает Emotet. Это ПО распознает отдельные характеристики в контексте своих знаний о «слоне» (то есть о троянской программе Emotet).

Если ПО обнаруживает подозрительную загрузку данных и планирование удаленной задачи, эти два инцидента могут не расцениваться как угроза. Но когда одновременно с ними распознается вредоносное вложение на сервере электронной почты, становится очевидно, что это атака с использованием Emotet. Благодаря технологии контролируемого обучения NSX Advanced Threat Analyzer сопоставляет различные данные и принимает решения.

Атака №2. Mirai

Ботнет **Mirai** — один из самых неприятных вирусов. Очень многие подверглись этой атаке, и почти для всех она стала неожиданностью.

Этот ботнет был образован из устройств Интернета вещей, включая персональные вычислительные устройства, камеры, термостаты и даже умные дверные звонки. Вредоносное ПО удаленно устанавливалось на любые устройства с ядром ОС UNIX.

Из-за ботнета Mirai организации утратили доступ к таким приложениям, как Twitter и Netflix, а также к важным бизнес-системам, включая системы промышленной автоматизации и контроля доступа. Какой из типов ИИ мог бы распознать готовящуюся атаку с использованием ботнета Mirai?

В ПО NSX Network Detection and Response используется неконтролируемое машинное обучение. Модуль ИИ непрерывно обучается, отслеживая данные в Интернете и обычный вертикальный и горизонтальный трафик.

Чтобы представить это более наглядно, проведем аналогию с кошками. Кошки бывают разных пород, разной окраски и разного размера, но все они имеют одинаковые признаки, характерные для кошек. Система распознает «эталонную» кошку, но не знает, хорошая она или плохая.

Эксперты в области ИИ называют отклонения от эталонных данных дрейфом. Представьте, что в поле зрения системы появились несколько собак или один тигр. У них есть общие характеристики, такие как шерсть и усы, но это разные животные.

Так распознаются аномалии. Система не может определить, насколько опасны эти аномалии, но она точно знает, что такие отклонения требуют дальнейшего анализа. Если изменения незначительные, система может не распознать их как вредоносную атаку.
Злоумышленники могут намеренно «засорить» данные обучения таким образом, чтобы аномальная активность выглядела как нормальная. Это так называемое **вредоносное машинное обучение**.

VMware NSX Network Detection and Response анализирует нормальный поток трафика от службы, собирающей данные с устройств Интернета вещей, и следит, чтобы этот трафик был входящим для диспетчера устройств Интернета вещей. В ПО NSX Network Detection and Response также используется неконтролируемое машинное обучение, которое позволяет провести анализ вредоносной среды и выявить непропорциональные объемы трафика, передаваемые в различных направлениях, в том числе на устройства, не прошедшие аутентификацию в концентраторе Интернета вещей.

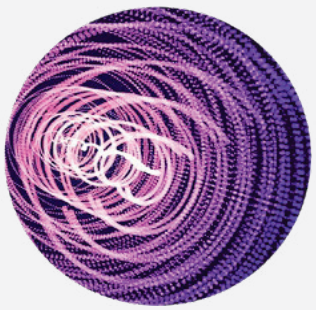
Хороший пример аномального трафика — двунаправленный трафик термостата, подключенного к Интернету. Пользователь периодически обновляет температуру, но в большинстве случаев от устройства поступают только данные телеметрии. Во время внезапной атаки Mirai это поведение изменилось, и устройство стало передавать намного больше трафика в нетипичном направлении.

ПО NSX распознает такую активность как подозрительное сканирование портов. Почему устройство Интернета вещей так себя ведет? NSX Network Detection and Response обнаруживает ботнеты Mirai, поскольку неконтролируемое машинное обучение позволяет распознавать активность, отличную от установленных эталонных данных.

Атака №3. LokiBot

LokiBot — это троянская программа для кражи учетных данных, которая может устанавливаться на платформе Windows, но чаще всего используется для атак на устройства Android. Она регистрирует активность пользователя, включая нажатия кнопок на телефоне или другом устройстве Android и нажатия клавиш на клавиатуре компьютера.

Атаки LokiBot можно предотвратить с помощью биометрической или двухфакторной аутентификации, но эти технологии используются не во всех приложениях и не на всех устройствах. Например, в марте 2017 г. вредоносная программа LokiBot была предустановлена на множество смартфонов и планшетов со стандартной операционной системой Android, которые были проданы ничего не подозревающим пользователям. Как можно было защититься от этого?



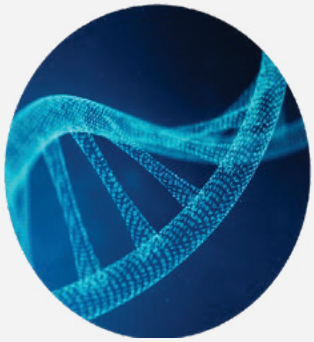
ИИ — идеальная технология для обнаружения LokiBot, поскольку она позволяет одновременно использовать контролируемое и неконтролируемое машинное обучение. Представьте себе ускоритель заряженных частиц, например Большой адронный коллайдер ЦЕРН, где частицы сталкиваются на огромной скорости. Такое столкновение приводит к рассеиванию атома и выделению его составных компонентов. Иногда возникают непредвиденные аномалии в виде побочных частиц. Таких скрытых аномалий быть не должно. Кроме того, могут появиться верные признаки некоторых атомных элементов. В подобных ситуациях используются оба типа ИИ: контролируемое машинное обучение для обнаружения ожидаемой активности и неконтролируемое машинное обучение для обнаружения аномалий.

Как работает ИИ в случае с LokiBot? Благодаря технологии неконтролируемого машинного обучения NSX Network Detection and Response распознает аномалии и отклонения от эталонных параметров. Кроме того, это ПО обнаруживает аномальное поведение с помощью алгоритмов, основанных на контролируемом машинном обучении. В сочетании с NSA ATA это ПО обнаруживает сходство с известными вредоносными объектами, например с сегментами кода, которые уже были замечены в клиентской базе NSX. ПО анализирует файлы, обнаруживает элементы горизонтального трафика и ищет признаки вредоносной активности, например сегменты кода (повторно используемые сторонние составные компоненты) из более ранних атак. Это элемент контролируемого ИИ.

Для обнаружения LokiBot требуется комбинация контролируемого и неконтролируемого машинного обучения. Ни одна из этих технологий по отдельности не решает эту задачу.

Атака №4. DMSniff

Многие стали жертвами **DMSniff** — установщика POS-теминалов. Эта программа размещается на устройствах, которые используются для повседневных платежей в магазинах, на заправочных станциях, в ресторанах и других местах. Программу DMSniff не удавалось обнаружить более четырех лет, и от нее пострадало множество розничных компаний. Для борьбы с DMSniff требуется сочетание глубинного обучения и контролируемого машинного обучения.



Механизм обнаружения DMSniff можно объяснить на примере телесериала «Детектив Раш». Детектив должен разобраться с нераскрытыми делами, а у полиции есть образцы ДНК, взятые на месте преступления. Анализ ДНК позволяет с высокой точностью установить личность преступника, однако он не дает результата, если в базе данных не найдено совпадений с взятыми образцами ДНК.

Несколько лет назад произошло знаковое событие — появилась компания 23andMe. Эта и другие подобные компании предлагают наборы для проведения генетических тестов на дому, с помощью которых любой человек может точно определить структуру своей ДНК, а также узнать, как выглядели его предки и насколько он подвержен определенным заболеваниям. Миллионы людей уже сделали такие тесты, благодаря чему значительно расширилась база ДНК. Теперь, когда полиция ищет подозреваемых по базе ДНК, она получает если не точные, то очень близкие совпадения. С помощью технологий ИИ, таких как глубинное обучение, полиция может сравнить образцы ДНК, взятые на месте преступления, с добровольно пополняемой базой данных 23andMe и с большой вероятностью найти родственников подозреваемого. Даже если не найдено 100-процентных совпадений, ИИ позволяет следователям найти членов семьи, к которой, возможно, принадлежит подозреваемый.

В среде хакеров широко распространено повторное использование кода. Хакеры активно взаимодействуют друг с другом и делятся элементами кода и процедурами, которые доказали свою эффективность. Такие фрагменты кода имеют четкие отличительные признаки или характеристики.

В случае с DMSniff применяется именно такой принцип, благодаря чему средства ИИ в составе NSX Advanced Threat Analyzer обнаруживают эту вредоносную программу. ПО обнаруживает обфусцированный трафик в DMSniff, поскольку командный и управляющий (сигнальный) трафик в основном содержит данные о нажатиях клавиш или данные банковских карт. Это тот самый повторно используемый элемент кода, который повторяется снова и снова. Даже если совпадение неточное, признаки очевидны.

Контролируемое машинное обучение, используемое в ПО NSX Network Detection and Response, позволяет обнаружить такие известные угрозы, как создание вредоносных доменов и эксфильтрация данных по каналам с низкой пропускной способностью. В сочетании с глубинным обучением эта технология позволяет проанализировать активность на наличие признаков DMSniff и принять своевременные меры.

Атака №5. Облачные рабочие нагрузки

У многих сложилось впечатление, что рабочие нагрузки в публичном облаке защищены лучше, чем в традиционных локальных вычислительных системах или частных облаках.

Это могло бы быть правдой, если бы компании не переносили в публичное облако огромное количество рабочих нагрузок, в том числе крайне важных для бизнеса; такие сценарии повышают риск кибератак. История бюро кредитных историй Equifax — возможно, один из самых ярких и известных примеров с самыми значительными последствиями.

Часть вертикального трафика в публичном облаке приходится на вычислительные платформы, такие как AWS, Azure или GCP, а другая часть — на интерфейс периметра. Различные виды аномальной активности возникают как во внутренних каналах, так и на периметре сети.

Однако основная сложность заключается в том, что не все аномалии представляют угрозу и не все угрозы аномальны. Вот почему недостаточно просто обнаружить аномалии. Они должны распознаваться в контексте.

Предположим, что установлено подключение к нетипичному порту. Это аномалия и характерный признак вредоносной активности в публичной облачной среде, однако это не обязательно атака. В этом заключается проблема обнаружения аномалий. При обнаружении аномалий наблюдается большое количество ложных срабатываний.

NSX Network Detection and Response проверяет наличие аномалий в журналах VPC, а также анализирует их в контексте, с учетом типа трафика и элементов вертикального трафика. Сопоставив полученные данные с закономерностями вертикального трафика на периметре облака, можно с уверенностью сказать, что обнаруженная аномалия опасна и совершена атака на экземпляр публичного облака в гибридной вычислительной среде.

В ПО NSX Network Detection and Response используются средства ИИ для выявления аномальной активности, связанной с атаками и являющейся частью атаки. Анализ контекста позволяет отличить отдельные ложные срабатывания от настоящих угроз.

Итог. Не верьте распространенным мифам об ИИ

Несмотря на то, что ИИ имеет свои ограничения и часто воспринимается как нечто экзотическое и бесполезное, при правильном применении он дает очевидные преимущества.

В конечном счете эффективная система кибербезопасности основывается на использовании различных типов ИИ. Каждый из этих типов выполняет определенную задачу, а все вместе они позволяют получить полную картину активности в сети и обнаружить атаки.

С учетом того, что более 70% всех сообщений электронной почты являются спамом, 50% трафика в Интернете порождают боты, а 40% этого трафика представляют собой вредоносную активность, специалистам по безопасности еще долго придется бороться с атаками.

Современные системы безопасности обеспечивают стабильную работоспособность вычислительных сред, возможность применять средства анализа для упрощения работы специалистов и пользоваться всеми преимуществами Интернета и вычислений.

ИИ — неотъемлемая часть таких систем, но важно понимать его возможности и ограничения. ИИ позволяет обнаруживать сложные угрозы и оптимизирует работу отделов безопасности, однако следует помнить о различиях технологий ИИ. Различные типы ИИ обеспечивают различные уровни защиты. Надлежащее использование ИИ в области кибербезопасности позволяет усилить контроль и сосредоточиться на более важных корпоративных задачах, чем поиск угроз.

В ПО NSX Network Detection and Response и NSX Advanced Threat Analyzer используются новейшие достижения науки о данных, позволяющие применять ИИ для обеспечения кибербезопасности. Этот подход к кибербезопасности стал результатом сотрудничества двух ведущих исследователей мирового уровня. ИИ — один из важнейших компонентов предлагаемого решения. С его помощью можно анализировать активность в сети и распознавать реальные угрозы, не пытаясь оградить всю сеть и предугадать возможные действия злоумышленников.