ПРИМЕНЕНИЕ АЛГОРИТМОВ МАШИННОГО ОБУЧЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ АНОМАЛИЙ В СЕТЕВОМ ТРАФИКЕ ИНФОРМАЦИОННЫХ СИСТЕМ

Вдовина А.Н.,преподаватель,

научный руководитель,

Павленко В.В., курсант 2 курса,

Уфимский юридический институт МВД России,

г. Уфа, Россия

Аннотация. В работе рассматривается возможность использования алгоритмов машинного обучения для поиска нетипичной и потенциально опасной активности в сетевом трафике информационных систем. Показано, почему традиционные сигнатурные средства защиты перестают успевать за современными способами атак и чем полезен переход к поведенческому анализу. Описаны особенности подготовки сетевых данных, основные группы применяемых алгоритмов и реальные сложности, с которыми сталкиваются при их внедрении в действующую инфраструктуру. А также

авторами отмечено, что совместное использование сигнатурной фильтрации и моделей машинного обучения приводит кнаиболее устойчивому результату.

Ключевые слова: машинное обучение, сетевой трафик, аномалии, кибератаки, информационная безопасность.

Каждая современная информационная система обменивается данными как внутри локальной сети организации, так и с внешними узлами, причем постоянно [5]. Значительно увеличилась и нагрузка на средства защиты информации, параллельно с ростом числа веб-сервисов, облачных хранилищ и удаленных рабочих мест. Долгое время основным барьером от сетевых угроз оставались межсетевые экраны и системы обнаружения вторжений, построенные на сигнатурном анализе. Принцип их работы довольно понятен: администратор поддерживает базу шаблонов уже известных атак, а анализатор сопоставляет с ней проходящие пакеты [2]. Сигнатуры срабатывают почти мгновенно и редко ошибаются в то время, как нарушители используют старые, хорошо изученные инструменты.Но жесткое правило перестает совпадать, если злоумышленнику стоит слегка изменить структуру пакета, или замаскировать полезную нагрузку, или воспользоваться новой уязвимостью.Вторжение проходит мимо системы защиты.

В связи с этим ограничениемвсе чаще переходят от поиска конкретных сигнатур к выявлению сетевых аномалий в задачах информационной безопасности. Система изучает привычное, нормальное состояние конкретной сети,вместо того чтобы пытаться перечислить все возможные варианты атак (логика здесь обратная) [6]. Ведется учет объема передаваемых данных, времени активности пользователей, соотношения протоколов и набора обычных портов. При этом резкие отклонения от этой картины отмечаются как подозрительные. Крайне трудно в практической деятельности настроить через фиксированные пороги такой контроль вручную.Редко бывает ровнойсетевая нагрузка.Работники одновременно в начале рабочего дня заходят в корпоративные системы, запускается резервное копирование баз данныхночью, идет в конце месяца массовая выгрузка отчетов. При установлении жестких границ дежурный

специалист разбирать ложные тревоги быстро устанет. При ослаблении границскрытое сканирование сети или медленная утечка файловостанутся незаметными.

Алгоритмы машинного обучения помогают решить такую задачу. Они способны самостоятельно находить в больших массивах журналов и сетевых соединений неочевидные закономерности. Сырой трафик, который перехватили прямо с сетевой карты, почти никогда не подают в модель, так как объем его слишком велик для быстрой обработки. Пакеты предварительно собирают по протоколам вроде NetFlow или
IPFIX
в сетевые потоки, затем переводят в набор числовых признаков [1]. Сюда попадают длительность сессии, частота служебных флагов
TCP
, количество отправленных и принятых байтов, паузы между соседними пакетами, разброс портов и адресов назначения. Грамотная очистка данных и выбор действительно показательных признаков нередко влияют на качество обнаружения сильнее, чем усложнение самого алгоритма, как показывает опыт разработки подобных систем.

В сетевом анализе используют несколько групп методов (в зависимости от наличия поставленной задачи и размеченных данных).В первую группу входит обучение с учителем.На заранее подготовленной выборке, где каждый сетевой поток уже отнесен к нормальному трафику или к конкретному классу угроз,тренируют модель [3]. Ансамбли деревьев решений (случайный лес и градиентный бустинг, метод опорных векторов)на достаточном уровне зарекомендовали себя. Они сохраняют сравнительно низкий процент ложных срабатываний при уверенном отделении штатной работы от подбора паролей, сканирования портов и DDoS-трафика.Вручную разметить реальный трафик крупной сети - очень долго и дорого. В этом и есть главная трудность такого подхода. Классификатор с учителем плохо реагирует на принципиально новые атаки, с которыми раньше не сталкивался, поскольку привязан к примерам из обучающей выборки [1].

Второе направление — обучение без учителя.Оно позволяет обойтись без ручной разметки инцидентов. Алгоритмы (изолирующий лес, одноклассовый метод опорных векторов, методы кластеризации) настраиваются на массиве обычного трафика и очерчивают границы привычного поведения сети [3]. Любое соединениепомечается как выброс, если выбивается сильно из плотных групп данных. Такой подход дает шанс заметить нетипичные угрозы вроде скрытой активности вредоносной программы, которая передает данные наружу в нерабочее время. Повышенная чувствительность к любым безобидным изменениям в инфраструктуре является минусом.Алгоритм воспринимаеткак инцидент безопасности подключение нового корпоративного сервиса или массовое обновление операционных систем.

К следующей группе относятся методы глубокого обучения. Их применяют,когда нужно уловить сложные нелинейные связи или растянутые во времени сценарии атак [4]. Выделяются нейросетевые автоэнкодеры: сеть учится сжимать вектор признаков нормального соединения и заново восстанавливать его с минимальной погрешностью. Ошибка восстановления резко растет, еслина вход поступает аномальный поток. Для системы мониторинга это и служит сигналом. Когда каждый отдельный запрос выглядит допустимым, но вся последовательность указывает на попытку взлома, удобны рекуррентные нейросети (для анализа цепочек событий во времени).Но сложнее всего внедряютсяименно глубокие модели.Они дольше обучаются и плохо поддаются объяснению, требуют серьезных вычислительных ресурсов. Поэтому специалисту понять, почему именно конкретный узел попал под подозрение,непросто.

Даже удачно подобранный алгоритм сталкивается с рядом технических препятствий при переносе из учебного эксперимента в реальную информационную систему. Прежде всего это сильный дисбаланс классов: в обычном сетевом трафике вредоносных соединений очень мало — обычно меньше 1%, а нормального трафика подавляющее большинство [6]. Привычная оценка по общей доле верных ответов в таких условиях перестает отражать реальность, ведь модель может вообще не замечать атаки и все равно показывать результат выше 99%. Поэтому ориентируются на полноту

обнаружения, точность срабатываний и их сбалансированный показатель -F1-меру - при настройке и тестировании [3]. Чтобы система не пропускала опасные события, разработчику приходится искать компромисс. При этом она не должна перегружать потоком пустых уведомлений службу безопасности.

Массовое использование шифрования по протоколам TLS и HTTPS- следующая серьезная проблема[5]. Модели приходится делать выводы только по внешним метаданным (длине пакетов, временным задержкам, характеристикам установки соединения и статистике заголовков), поскольку содержимое пакетов скрыто от анализатора. Не менее важен и дрейф данных (постепенное изменение самой сети). Со временем в организации появляются новые серверы, меняются привычки пользователей и состав рабочих приложений. Если алгоритм обучить один раз и больше не обновлять, его точность со временем снизится. Поэтому систему сразу проектируют с регулярным дообучением на свежих проверенных журналах [6].

С учетом всех плюсов и ограничений в пользу одного лишь машинного обучения на практике почти никогда не отказываются от классических средств защиты. При этом комбинированная схема работает надежнее.Быстрый сигнатурный модуль сразу отсекает массовые известные атаки еще на первом уровне и снимает лишнюю нагрузку с серверов.На втором уровне поведенческие алгоритмы проверяют оставшийся трафик на скрытые аномалии [1]. Вдобавок используется каскадная проверка. Отбирает сомнительные сессии простой детектор выбросов, а отфильтровывает случайные всплески пользовательской нагрузки более точный классификатор. В конечном итоге полностью машинное обучение администраторов безопасности не заменяет, но становится удобным рабочим вспомогательным инструментом, замечающим нетипичную активность еще до того, как она приведет к сбою сервисов или утечке данных.

Литература

1. Браницкий А.А., Котенко И.В. Анализ и классификация методов обнаружения сетевых атак // Труды СПИИРАН. 2016. № 2 (45). С. 207–244.

2. Лукацкий А.В. Обнаружение атак. 2-е изд. СПб.: БХВ-Петербург, 2003. 596 с.

3. Мюллер А., Гвидо С. Введение в машинное обучение с помощью Python. Руководство для специалистов по работе с данными / пер. с англ. М.: Вильямс, 2017. 393 с.

4. Николенко С., Кадурин А., Архангельская Е. Глубокое обучение. Погружение в мир нейронных сетей. СПб.: Питер, 2018. 480 с.

5. Олифер В.Г., Олифер Н.А. Компьютерные сети. Принципы, технологии, протоколы: учебник для вузов. 5-е изд. СПб.: Питер, 2016. 992 с.

6. Шелухин О.И. Сетевые аномалии. Обнаружение, локализация, прогнозирование. М.: Горячая линия – Телеком, 2019. 448 с.