Безопасность

Как мы применяем машинное обучение в решениях Cisco для защиты от сложных угроз

Джо Маленфент (Joe Malenfant)
1 августа 2018 г. – 0 комментариев

Последнее время в области сетевой безопасности много говорят о машинном обучении. Похоже, нельзя вести разговор о чем-то одном, не упоминая другого. Многие организации, с которыми я общался за последние несколько месяцев, заинтересованы в получении более подробной информации, но, начиная изучение, часто приходят в еще большее замешательство. Хороший пример – Раскрытие мифов о машинном обучении в области безопасности оконечных устройств.

В Cisco машинное обучение используется уже на протяжении десятилетий, так что для нас эта тема не нова. Только в области безопасности у нас работает множество команд, и более 20 сотрудников имеют ученые степени в сфере машинного обучения. Наши рабочие группы используют машинное обучение как средство для обнаружения и анализа угроз. Это способ, а не результат. В области информационной безопасности это важное различие. В последние несколько лет мы наблюдали, как многие компании рекламируют свои системы машинного обучения, но они никогда не объясняют, что это означает в действительности.

Чем отличается Cisco?

В 2013 году мы приобрели Cognitive Security, компанию, которая занималась исключительно машинным обучением. Мы быстро интегрировали их технологию (теперь она называется Cognitive Intelligence) с нашими решениями для обеспечения безопасности веб-

трафика, чтобы улучшить обнаружение угроз (см. блоги). Это был пассивный подход к обнаружению угроз. Журналы отправляются с прокси-сервера в Cognitive Intelligence для анализа. Мы анализируем параметры, записанные в журналах, чтобы обнаружить аномальную активность; анализировать полезные данные для этого нам не нужно. Результат прост. Cognitive Intelligence предупреждает только о хостах, которые можно однозначно определить как скомпрометированные. Так как решение указывает только на подтвержденные случаи заражения, аналитики не тратят времени впустую и могут сразу переходить к восстановлению и очистке.

Это стало только началом внедрения машинного обучения в наш портфель решений для обеспечения безопасности. Мы быстро осознали ценность этой технологии и начали использовать ее мощные возможности аналитики и в других компонентах стека решений для обеспечения безопасности. Мы включили алгоритмы для сопоставления больших объемов данных и предоставления аналитики за рамками того, что можно разглядеть с одного направления. Например, если вы можете сопоставить данные сетевого трафика с исходящими соединениями прокси для выявления скомпрометированного хоста, имеющего права администратора и осуществляющего горизонтальное распространение угрозы, это было бы невозможно обнаружить с помощью одной технологии. Однако это можно было бы сделать, если объединить несколько фрагментов картины. И именно в этой области мы осознали истинную ценность того, что у нас было.

Машинное обучение в применении к телеметрии сети

Компания Cisco широко известна как новатор в области коммутаторов и маршрутизаторов. По сути мы создали опорную сеть для Интернета и инфраструктуры большинства организаций. Эта имеющаяся сетевая инфраструктура является богатым источником данных. Например, Stealthwatch собирает и анализирует телеметрию сети, чтобы выявлять неявные угрозы. Это решение также интегрируется с механизмом машинного обучения Cognitive Intelligence, который сопоставляет наблюдаемые **локально** на предприятии характеристики угроз с их **глобальным** поведением. Оно может обнаруживать аномалии и является достаточно интеллекутальным, чтобы затем классифицировать отдельные фактические фрагменты «активности угрозы» (потому что аномальное не

обязательно должно быть вредоносным), обеспечивая критически важные оповещения с высокой достоверностью. Эта технология также лежит в основе решения Encrypted Traffic Analytics (ETA), которое может обнаруживать вредоносное ПО в зашифрованном трафике *без расшифровки*, впервые в отрасли!

Машинное обучение в области безопасности оконечных устройств

При обсуждении обеспечения безопасности оконечных устройств широко признается, что обнаружение на основе сигнатур (например, хеш-сумм файлов) является частью решения, но не ПОЛНЫМ решением. Не так сложно изменить значения хеш-суммы файла или диапазон IP-адресов, а это значит, что злоумышленники могут создавать новые хеш-коды SHA256 для каждого случая заражения. Хотя значения хеша может быть достаточно для выявления отдельного вредоносного файла, это не поможет выявить другие связанные заражения полиморфными вредоносными программами, которые могут быть связаны с той же уязвимостью и даже с тем же злоумышленником. Одна и та же хеш-сумма просто никогда не встретится дважды.

Применяя машинное обучение к этим файлам, мы способны разобрать каждый из них на фрагменты. Это как рассматривать отдельные компоненты, из которых состоит автомобиль, а не весь автомобиль целиком. Да, в автомобиле есть шины, двигатель, ветровое стекло, окна, рама и т. д. Но очевидно, что не все автомобили одинаковы. То же самое верно и для вредоносных программ. Мы может разобрать каждую отдельную угрозу на мельчайшие фрагменты (более 400 различных атрибутов). Эти атрибуты используются в качестве дискретных классификаторов в модели машинного обучения. Более высокий уровень детализации ведет к более интеллектуальному, лучше обученному алгоритму и более высокой точности результатов. Это означает, что наше машинное обучение лучше справляется с выявлением новых и видоизмененных угроз. Хакеры часто переупаковывают свои средства использования уязвимостей в различных форматах, например уязвимость во Flash из CVE-2018-4878, которая использовалась в нескольких эксплойтах, включая ROKRAT и его последующую кампанию. Машинное обучение — это одна из 14 различных методик, которые используются в решении AMP for Endpoints для обнаружения угроз и защиты от них.

Объединение всех фрагментов

Одним из способов, которые мы используем в Cisco, является определение моделей хакера с помощью машинного обучения и аналитического механизма Cognitive Intelligence. Сопоставляя данные телеметрии из журналов веб-прокси (Cisco и сторонних), телеметрию сети (из Stealthwatch), значения SHA256 и характеристики файлов из AMP, он определяет, как действуют злоумышленники, что они делают и даже кто они. Отправляя весь этот объем данных в наши алгоритмы машинного обучения, мы обеспечиваем непревзойденный уровень обнаружения, а самое главное, блокируем большую часть угроз, прежде чем возникнут серьезные проблемы. В будущих блогах мы подробно рассмотрим различные классификаторы.

Вы можете ознакомиться с работой решения AMP for Endpoints самостоятельно с помощью бесплатной пробной версии, которая доступна по этому адресу: www.cisco.com/go/tryamp.

Чтобы подробнее узнать о том, как мы применяем машинное обучение в решениях Cisco для обеспечения безопасности, просмотрите этот технический видеоролик.

Теги:

Защита от сложного вредоносного ПО
Решения для защиты от сложных угроз
Защита оконечных устройств
Машинное обучение

Для того чтобы не затягивать обсуждения, комментарии в блогах Cisco закрываются через 60 дней после публикации. Посетите сайт блогов Cisco для получения актуальной информации.