Машинное обучение против неизвестных угроз

Сергей Невструев – менеджер по развитию бизеса, компания Check Point Software Technologies.

Угрозы становятся динамическими

Особенность современных угроз, связанных с информационной безопасностью компаний, в том, что они постоянно меняют свой облик. Их все сложнее выявлять по каким-то статическим признакам: сигнатурам, IP-адресам, доменным именам, URL и т.д. Более того, это становится общей особенностью всех угроз, включая массовые рассылки, а не только особенностью таргетированных заказных атак.

Цикл атаки может включать:

– социальную инженерию и профилирование жертвы;

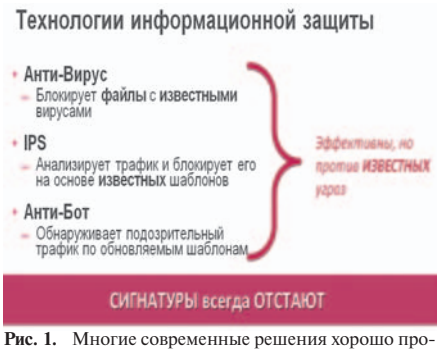

Рис. 1. Многие современные решения хорошо противостоят только известным угрозам, выявляемым по сигнатурам.

Рис. 2. Статистика показывает,что большинство вирусов встречается лишь один раз.

– вредоносные или скомпрометированные популярные веб-сайты, целевые фишинговые электронные письма, которые обеспечивают доставку вредоносного контента;

– вредоносные файлы, которые загружаются на станцию жертвы;

– сложные сетевые взаимодействия между вредоносом на станции жертвы и командными серверами.

Текущие решения, представленные на рынке ИБ, очень хорошо блокируют атаки, связанные с уже известными угрозами в файлах или сетевом трафике на основе известных паттернов. К ним относятся (рис. 1):

– *анти-вирусное ПО* – блокировка файлов с известным вредоносным кодом по сигнатурам *на уровне шлюзов и конечных станций*;

– *IPS* – анализ трафика и его блокировка на основе известных шаблонов атак;

– *анти-боты* – обнаружение и блокировка подозрительного трафика от скомпрометированных станций по обновляемым шаблонам взаимодействия (паттернам) и адресам (IP, FQDN) командных серверов.

В настоящее время у злоумышленника есть множество способов менять атаку «на лету», в том числе автоматизированно. Переупаковщики, обфускация, генераторы кода, сложные алгоритмы вычисления новых доменных имен командных серверов делают блокировку угроз только по сигнатурам невозможной. Как показывает статистика, большинство экземпляров вредоносного кода встречается лишь один раз, а 99% контрольных сумм вредоносов видны 58 секунд или меньше *(ucm.: Verizon 2016 Data Breach Investigations Report)*. Чтобы избежать детектирования, хакеры модифицируют код и схемы взаимо-

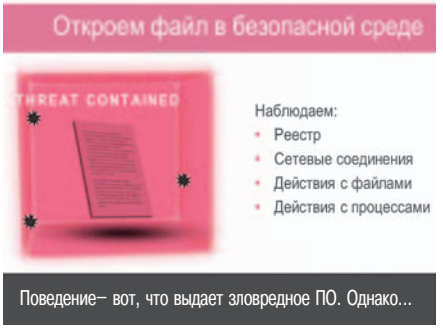

Рис. 3. Эмуляция поведения – один из основных способов определения вредоносности файла/документа.

действия для каждой новой атаки (рис. 2). И те решения, которые анализируют копию какого-то вредоноса и выпускают сигнатуру, чтобы заблокировать вторую копию, становятся неэффективными вследствие того, что второй копии может вообще не быть. Злоумышленник будет постоянно менять свой вредонос, и вредонос будет уникальным, например, в каждом фишинговом письме.

Эмуляция поведения и машинное обучение становятся основными компонентами решений ИБ

Философия Check Point состоит в том, чтобы любой вредоносный файл блокировать до того, как он попадет в ИТ-инфраструктуру и нанесет ущерб компании.

И здесь возникает вопрос: “Каким образом можно понять, что некий файл/документ – это вредонос”? Понимание достигается достаточно известным способом, которым антивирусные компании пользуются уже длительное время – эмуляцией, т.е., если вредонос должен сработать на машине пользователя, то лучше вызвать его срабатывание в безопасной среде – “песочни-

Рис. 4. Вечная борьба “добра со злом”: злоумышленники постоянно ищут способы противодействия решениям ИБ.

Рис. 5. Семейство решений Check Point для противодействия неизвестным угрозам (угрозам нулевого дня).

це". Соответственно, он не принесет вреда, но наблюдая за его поведением и за тем, что происходит с рабочей станцией – реестром, сетевыми соединениями, действия с файлами/процессами и др., можно выяснить является ли этот файл "чистым" или "вредоносным" (рис. 3).

Указанный способ оказался настолько эффективным, что злоумышленники стали искать пути обхода песочницы. Общий подход здесь состоит в том, что когда вредонос исполняется, он пытается определить: где он запущен – в контролируемой среде или на рабочей станции жертвы. Если устанавливается первый случай – вредонос никак себя не проявляет (рис. 4).

Как это можно сделать? *Первый* способ – запуск по таймеру: когда вредонос попадает в контролируемую среду, он не сразу начинает свою вредоносную активность, а с некоторой задержкой. Все помнят такой вирус: "чернобыль", который заразил десятки тысяч машин, и 26 апреля 1999 г. все они перестали работать. Производители "песочниц" ответили ускорением времени в операционной системе, но злоумышленник может реализовать свой собственный внутренний таймер и все равно обеспечить задержку исполнения, превышающую время эмуляции.

Второй и третий способы – это обнаружение "песочницы" или ожидание действий человека. "Песочница" – это такое же ПО, которое присутствует в виде файлов, процессов, ключей реестра. К этому можно добавить косвенные признаки, которые "песочницу" могут выдать, например, вредонос может опрашивать MAC-адреса сетевых карт и другие параметры аппаратного окружения. Противодействием этому может являться эмуляция аппаратного окружения, включая CPU, вредонос отвечает обнаружением эмуляции CPU, и т.д.

При *третьем* способе вредонос ожидает действий человека. Например, можно измерять скорость прокрутки документа. В первых "песочницах" документ быстро "прокручивался" до самого низа – злоумышленники стали это "отлавливать". Check Point обнаружил пример интересного документа MS Word с макросом. Это работало следующим образом: в середину документа была вставлена картинка неприличного содержания, соответственно: при просмотре этого документа человеком скорость скролинга менялась; когда скролинг происходил в "песочнице" этого не происходило. Таким образом, вредонос "понимал", что документ открыт не на настоящем компьютере, и не выполнял дальнейших действий.

Для того чтобы оградить компании своих клиентов от таких, более сложных, атак Check Point разработал семейство технологий, названное SandBlast (рис. 5), которые позволяют защищать компании от неизвестных угроз, или угроз "нулевого дня".

Первая – Threat Emulation – технология эмуляции, которая позволяет отлавливать вредоносы, какие бы способы обхода песочницы они не использовали.

Вторая технология – Threat Extraction (проактивное удаление опасного контента при доставке) – позволяет мгновенно очищать и доставлять документы, до того, как сделан вывод, опасен этот документ или нет, без влияния на продуктивность пользователей. Данная технология удаляет все потенциально опасное содержимое из документа, и в таком усеченном варианте доставляет его получателю. Возможно сохранение исходного формата или печать в PDF. Оригинал документа пользователь может получить, перейдя через несколько минут по ссылке, которая будет доступна в исходном письме только при подтверждении системой защиты безобидности оригинального файла. По статистике Check Point, более чем в 90% случаев пользователи не запрашивают оригинал документа, а довольствуются PDF-версией, что в совокупности с технологией Threat Emulation сводит на нет попытки доставки вредоносного кода, используя офисные форматы. Другие же типы файлов с высоким уровнем риска (исполняемые, скрипты и проч.) могут быть заблокированы на шлюзе безопасности по метаданным.

Третья технология – Endpoint Forensics – разработана для защиты рабочих станций и позволяет автоматически обнаружить,

Рис. 6. Основные компоненты решения Check Point для противодействия угрозам нулевого дня.

что рабочая станция заражена, изолировать ее и расследовать инцидент. Технология Endpoint Forensics дает возможность защитить рабочую станцию, если вредонос все же проник на нее, например, через USB-накопители. Благодаря тому, что данная технология выполняет запись в журнал всей подозрительной активности на рабочих станциях, во-первых, администратор безопасности может выявить заражение рабочей станции. Во-вторых, заблокировать либо процесс, либо компьютер целиком. В-третьих, автоматически собрать информацию, связанную с инцидентом, например, о том, каким образом вредонос проник на компьютер, как атака развивалась, и к каким данным был доступ, т.е. сразу понять, почему атака стала возможна и какой ущерб был нанесен. И, в-четвертых, выявить наличие аналогичных маркеров заражения на других компьютерах организации. Более того, можно задать действия необходимые для удаления вредоноса с зараженного компьютера.

Для полноты картины: *Zero Phishing* – защита учетных записей от кражи через фишинговые сайты и *Zero Ransomware* – идентификация и восстановление после действий программы-вымогателя или от программы-шифровальщика. Последняя технология позволяет: 1) понять, когда шифровальщик активен, 2) найти шифровальщика и заблокировать, 3) установить зашифрованные файлы и восстановить их в первоначальное состояние за счет автоматически сделанных резервных копий.

В контексте машинного обучения наиболее интересны технологии Threat Emulation и Endpoint Forensics. В первом случае именно на основе машинного обучения выносится вердикт о вредоносности документа в процессе его анализа. Во втором случае решение о блокировке процессов в ОС и изоляции рабочей станции также выносится на основе методов машинного обучения.

Эти технологии разворачиваются в следующих инфраструктурных компонентах (рис. 6): облаке – SandBlast cloud; стоечном сервере, который находится на площадке заказчика в датацентре – SandBlast Appliance; агентском ПО, которое ставится на конечные станции – ноутбуки, рабочие станции, планшеты и др. – SandBlast Agent.

Threat Emulation – "песочница"

Первый уровень, где применяется машинное обучение, это в "песочницах" – на стоечных серверах, где анализируется поведение файлов. Система защиты перехватывает файлы при загрузке их из Интернета или при пересылке их в качестве вложения в электронное письмо. Проверяемые файлы отправляются на эмуляцию в песочницу, которая представляет собой устройство Check point SandBlast Appliance, размещенное либо на площадке заказчика, либо в облаке, в зависимости от выбранного варианта решения. В некоторых случаях используется гибридный режим: документы, потенциально содержащие конфиденциальные данные, проверяются исключительно локально, остальные файлы (например, исполняемые) направляются в облако. По итогам проверки вредоносности файла, система эмуляции выдает вердикт: заражен

проверяемый файл или нет. В случае выявления вредоносной активности при запуске проверяемого файла пользователь получает подробный отчет об идентифицированной угрозе. И если заказчик не против обмена данными о найденных вредоносах, то "песочница" передает анонимную информацию об обнаруженной угрозе, включая контрольную сумму, веб-ссылку, сам вредоносный файл, в облачный сервис ThreatCloud, тем самым защитив от данной угрозы другие компании, использующие наши решения. Серверы SandBlast Appliance, используемые в качестве "песочницы" – это готовые решения, которые производит компания Check Point. При этом старшее устройство рассчитано примерно на обработку 2 млн. уникальных файлов в месяц. Младшее устройство способно анализировать 250 тыс. файлов в месяц. Если требуется обработка бОльшего числа файлов, организуется кластер из нескольких серверов, между которыми нагрузка автоматически балансируется. В серверах используются процессоры архитектуры Intel Haswell и более новые, которые поддерживают диагностику на уровне инструкций процессора. Этот функционал позволил Check Point создать уникальную технологию обнаружения новых эксплойтов – CPU-level exploit detection. Таким образом, вредоносные файлы могут быть обнаружены на ранней стадии исполнения еще до того, как они могут попытаться обнаружить или обойти «песочницу».

В результате анализа в «песочнице» на локальном устройстве и/или в облаке выявляются поведенческие характеристики/паттерны вредоносов, связанные с запуском процессов, скриптов, сетевой активностью, изменениями в реестре и др. По мере набора статистики по миллиардам проверенных «чистых» и вредоносных файлов формулируется база знаний и поведенческие правила, что, например, какая-то файловая операция или изменение какого-то конкретного ключа реестра чаще всего связаны с вредоносом, а другие операции, напротив, являются вполне легитимными.

Второй уровень, где применяется машинное обучение, это автоматизированное формирование сигнатур для файлов и сетевых взаимодействий, которые сами по себе хоть и не позволяют блокировать новые неизвестные угрозы, но существенно сокращают площадь атаки, блокируют обратные каналы связи с сервером управления и заставляют злоумышленников инвестировать больше средств в подготовку новых атак. При этом сигнатура должна быть сформирована таким образом, чтобы она реагировала на возможные вариации вредоноса, но при этом не затрагивала «чистые» файлы в сетях клиентов. Для этого новая сигнатура может "обкатываться" в фоновом режиме (без блокировки), собирается статистика по ее срабатыванию, она постепенно дорабатывается и переводится в основную базу.

В обоих случаях машинное обучение формирует базу новых правил и сигнатур, валидацию которых в дальнейшем проводят наши аналитики.

Endpoint Forensics – SandBlast Agent

Третий уровень использования машинного обучения – на рабочих станциях. Хотя веб-доступ и электронная почта по-прежнему являются основными источниками заражения, но далеко не все векторы доставки вредоносного кода можно контролировать на уровне сети: пользователь может скачать файлы на станцию через внешний USB-накопитель; получить файл в зашифрованном архиве, а пароль к нему может быть направлен в графическом изображении в письме, отдельным письмом или по SMS). Поэтому некоторый аналог «песочницы» в виде SandBlast Agent находится непосредственно на рабочей станции. В его задачи входит не только применение сигнатур, не только изоляция (блокировка) скомпрометированной станции, но и поведенческий анализ того, что происходит в самой операционной системе на станции, а также отправка в "песочницу" (локальную или облако) новых файлов, которые попали на рабочую станцию в обход шлюза безопасности. И как только поступает положительный вердикт на пересланный файл (он признан вредоносным), агент автоматически выстраивает цепочку всех событий, которые произошли с момента первоначального заражения, формирует сведения о нанесенном ущербе – т.е. он обеспечивает автоматическое расследование инцидента. Это существенно снижает затрачиваемое время на решение инцидента и требования к квалификации персонала (рис. 7). Кроме того, агент самостоятельно применяет правила поведенческого анализа непосредственно на самой станции, которые точно так же, как и для "песочницы", пополняются обновлениями из облака.

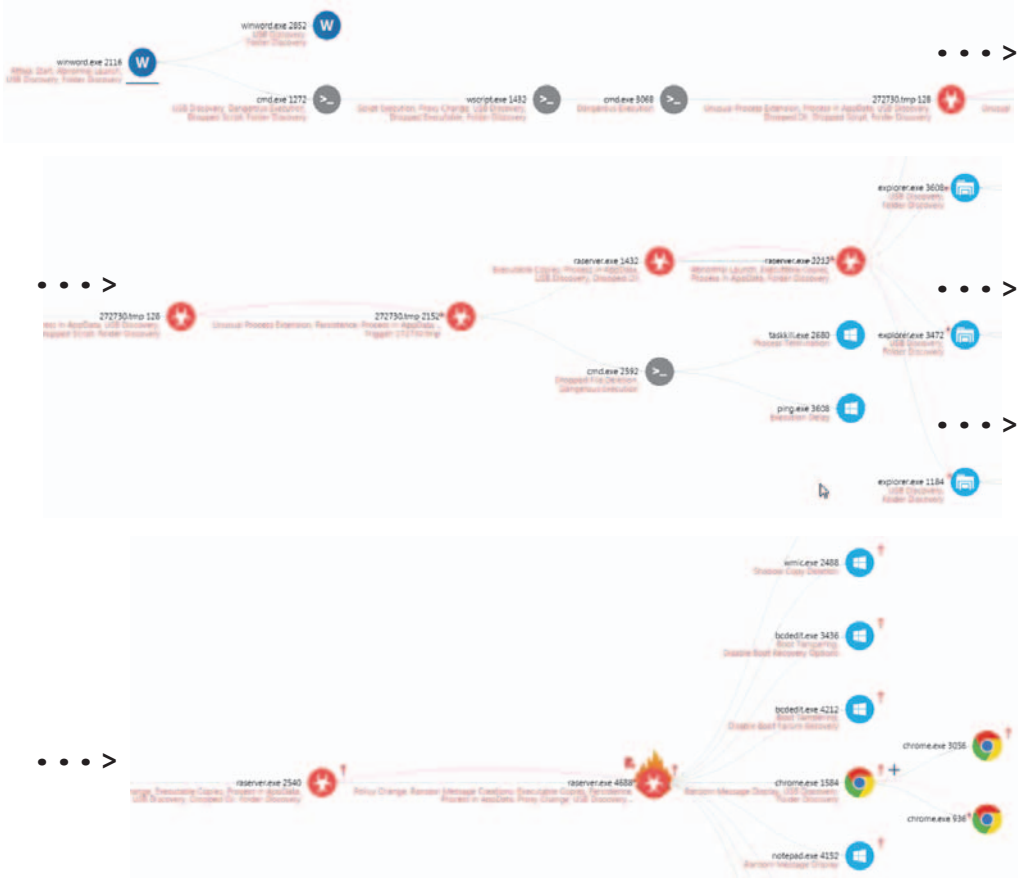

Рис. 7. Автоматическая цепочка событий (слева направо, сверху вниз) формируемая агентом, при проникновении зловреда на рабочую станцию.

Заключение

В итоге на практике суть машинного обучения при противодействии неизвестным угрозам можно представить следующими тремя этапами/уровнями. Первый – "песочница" – обладает некими первоначальными знаниями (заданными экспертами производителя) о том, что некоторые поведенческие характеристики свойственны вредоносному коду. Второй – "песочница" эмулирует новые неизвестные файлы, из которых выделяются вредоносные. Новые вредоносы, помимо известных, продемонстрировали и другие характеристики поведения/паттерны, что учитывается в общей статистике (от заказчиков и аналитической лаборатории Check Point). Это является источником новых правил. Кроме того, такой высокий уровень защиты применяется и на уровне сети, и на уровне рабочей станции. Третий уровень связан с обогащением новыми сигнатурами. Источником новых сигнатур являются движки автоматического анализа и "песочницы". После генерации сигнатуры проходят валидацию специалистами Threat Intelligence. Некоторые сигнатуры также тестируются в фоновом режиме, чтобы исключить ложные срабатывания и влияние на доступность сервисов.

Такой уровень автоматизации является необходимым для эффективного противодействия современным угрозам и позволяет быть на шаг впереди злоумышленников.

Сергей Невструев,
компания Check Point Software Technologies.