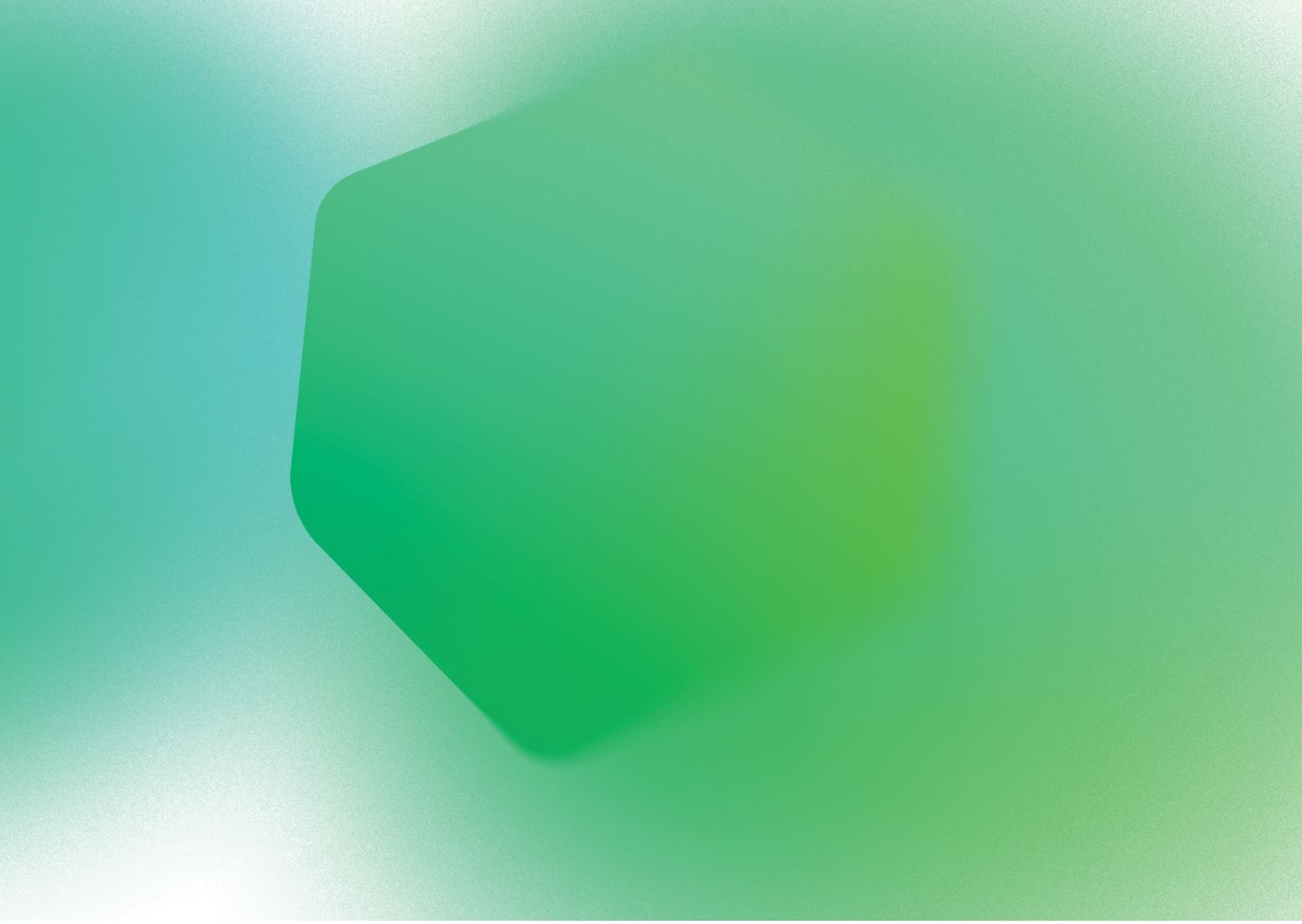

Системный подход к защите от сложных и целевых атак

Kaspersky MDR: охота на охотников

kaspersky

Подробнее на сайте kaspersky.ru
#активируйбудущее

Введение

По мере того как автоматизируются корпоративные процессы, бизнес все больше полагается на информационные технологии. Это значит, что риски, которые могут повлечь нарушение ключевых бизнес-процессов, смещаются в IT-сферу. Разработчики инструментов автоматизации знают об этом и, чтобы минимизировать угрозу, увеличивают инвестиции в IT-безопасность – ключевую характеристику любой IT-системы наряду с надежностью, гибкостью и стоимостью. За последние двадцать лет безопасность программных продуктов значительно улучшилась. Практически все производители ПО на мировом рынке теперь публикуют документы о безопасных конфигурациях и безопасном использовании своих продуктов, а ИБ-рынок насыщен разнообразными предложениями защиты.

С другой стороны, чем сильнее компания зависит от IT, тем привлекательнее для киберпреступников выглядит идея взломать ее системы. И это оправдывает вложения, необходимые для проведения успешной атаки на фоне повышения IT-безопасности.

Системный подход к защите

Повышение безопасности ПО и постоянное развитие защитных технологий осложняют организацию успешной атаки. Следовательно, киберпреступники, вложившие немало сил и ресурсов в преодоление нескольких уровней защиты, захотят находиться внутри атакуемой инфраструктуры как можно дольше, чтобы причинить максимум ущерба и извлечь максимум выгоды из атаки. Именно для этого и организуются целевые атаки.

Они планируются заблаговременно и реализуются с большой тщательностью. В ходе их проведения используются не только автоматизированные инструменты, но и навыки опытных киберпреступников. Дать им достойный отпор могут лишь профессионалы, обладающие не меньшей квалификацией и оснащенные современными инструментами для обнаружения и предотвращения атак.

С точки зрения управления рисками, считается, что организация достигла цели в области безопасности, если стоимость атаки для злоумышленника превышает потенциальную выгоду. А взломать несколько уровней защиты не только сложно, но и дорого. Тем не менее можно значительно сократить расходы на продвинутую атаку и при этом почти гарантированно избежать обнаружения встроенной защитой. Для этого злоумышленникам нужно только дополнить свой арсенал широко известными легитимными инструментами и методами.

Современные операционные системы фактически включают в себя все необходимое для того, чтобы их атаковать. Злоумышленникам не нужно использовать вредоносные программы, что существенно снижает затраты на успешную атаку. «Двойная функциональность» встроенных в ОС инструментов обусловлена тем, что их активно используют системные администраторы, поэтому отличить их легитимные действия от действий атакующих очень сложно – и практически невозможно с помощью одних только автоматических средств. Противостоять таким угрозам можно, только используя системный подход к защите (рис. 1). Он подразумевает, что, если угрозу нельзя предотвратить, она должна быть мгновенно обнаружена. Если же автоматическое обнаружение невозможно, необходимы проактивный поиск угроз и различные методы реагирования на инциденты. Собранные данные должны анализироваться, чтобы выявлять угрозы, избежавшие обнаружения автоматизированными системами защиты, и оперативно реагировать на них.

Рис 1. Системный подход к защите

Прячась у всех на виду

Мы в «Лаборатории Касперского» с достаточной степенью уверенности можем заявить, что внушительный список технологий обнаружения и предотвращения, которые мы создавали на протяжении многих лет (включая наши последние достижения в исследовании больших данных и машинного обучения), говорит о том, что наши защитные продукты способны нейтрализовать любую атаку, которую можно обнаружить и предотвратить автоматически. Но автоматическое обнаружение и предотвращение – это только начало. Более 20 лет исследований и предотвращения кибератак подарили нам еще более мощный инструмент, позволяющий добиться результата там, где не справляется автоматика, – наш бесценный опыт.

Целевые атаки разрабатываются с учетом особенностей защитных систем, используемых жертвами, чтобы обходить механизмы автоматического обнаружения и предотвращения угроз. Такие атаки зачастую проводятся вообще без использования ПО, а действия злоумышленников практически не отличаются от обычных действий ИБ- и IT-специалистов.

Ниже перечислены лишь некоторые приемы современных киберпреступников:

- Использование методов, затрудняющих цифровой криминалистический анализ, например безвозвратного удаления артефактов с жесткого диска или осуществления атаки исключительно в памяти компьютера
- Использование легитимных инструментов, которые обычно применяются в IT-отделах и службах информационной безопасности
- Многоэтапные атаки, когда следы ранее осуществленных действий безвозвратно удаляются
- Интерактивная работа команды профессионалов (аналогичная тестированию на проникновение)

Подобные атаки можно выявить только после того, как целевая система будет скомпрометирована, – только тогда можно обнаружить подозрительное поведение, указывающее на вредоносную активность. Именно поэтому крайне важно участие профессионального аналитика. Присутствие человека в цепочке анализа событий компенсирует недостатки логики автоматического обнаружения. Когда в атаке, подобной тестированию на проникновение, активно участвует сам злоумышленник, у него, естественно, есть преимущество перед автоматизированными технологиями защиты. В этом случае единственным надежным способом отразить угрозу становится личное вмешательство не менее квалифицированного аналитика.

Нехватка ИБ-специалистов

В ИБ-сфере сейчас наблюдается кадровый кризис. На текущий момент дефицит специалистов во всем мире – 4,07 миллиона сотрудников, в то время как в прошлом году он составлял 2,93 миллиона. Спрос на ИБ-экспертов растет, отыскать их становится все сложнее, а их услуги дорожают. Так что, если вашей компании не хватает специалистов по активному поиску угроз, расследованию инцидентов и реагированию на них, вряд ли можно рассчитывать, что вам легко и быстро их удастся нанять. Следовательно, нужно идти другим путем.

Продукты и сервисы категории Managed Detection and Response, или MDR («управляемые обнаружение и реагирование»), могут стать эффективным решением для организаций, желающих создать и усилить систему эффективного раннего обнаружения угроз и реагирования на них, но не располагающих достаточными внутренними ресурсами (рис. 2). Передача сложных задач безопасности, таких как активный поиск угроз, опытному поставщику сразу же повысит уровень ИБ-зрелости организации без найма и обучения сотрудников. Полностью управляемые персонализированные процессы обнаружения, приоритизации, расследования и реагирования помогут предотвратить простои и минимизировать ущерб от инцидентов, оправдав все вложения.

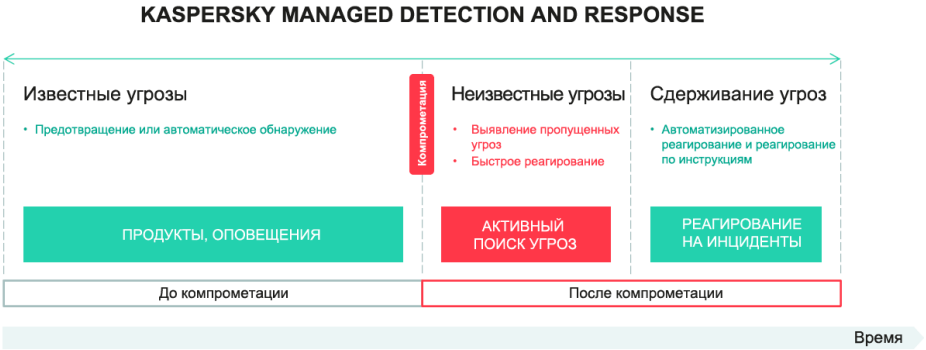

Рис. 2. Область применения MDR-сервисов

Иголка в стоге сена

SOC «Лаборатории Касперского» ведет непрерывный мониторинг более чем 250 тыс. конечных точек по всему миру, и их число постоянно растет. Мы собираем и обрабатываем огромное количество данных телеметрии, поступающих с каждого устройства. Основная масса угроз обнаруживается и предотвращается автоматически, и на проверку людьми отправляется лишь их малая часть. Тем не менее объем необработанных данных телеметрии, требующих дополнительного разбора, колоссален, и их ручной анализ в рамках сервиса активного поиска угроз попросту невозможен. Поэтому для дальнейшего рассмотрения аналитики SOC выбирают те необработанные события, которые так или иначе связаны с известной (или хотя бы теоретически возможной) вредоносной активностью.

Отбор таких событий (их официальное название – индикаторы атаки) в нашем SOC называют «охотой» – они помогают автоматизировать процесс поиска угроз. Создание индикаторов атаки – своего рода искусство, которое требует творческого подхода. Нужно задать правильные вопросы, например: «Какие техники важно обнаружить в первую очередь, а какие, напротив, могут немного подождать?» или «Какими приемами, скорее всего, воспользовались бы реальные злоумышленники?» – и получить на них ответы. В этом деле нам очень помогают знания методов киберпреступников.

Обнаружение на базе индикаторов атаки применяется после вторжения в случаях, когда сами инструменты атаковавших не являются вредоносными, а вот их использование – да. В ходе анализа выявляется подозрительное использование стандартных возможностей легитимных инструментов – автоматическая классификация такого поведения как вредоносного невозможна.

Примеры индикаторов атаки:

- **Запуск скрипта командной строки (или bat-файла / скрипта PowerShell) в браузере, офисном или серверном приложении (например, SQL Server, агент SQL Server, nginx, JBoss, Tomcat и т. д.)**
- **Подозрительное использование инструмента certutil для загрузки файла (пример команды: certutil -verifyctl -f -split https[:]//example.com/wce.exe)**
- **Выгрузка файла с помощью BITS (фоновой интеллектуальной службы передачи)**
- **Команда whoami из учетной записи SYSTEM и т. д.**

«Лаборатория Касперского» выявляет почти половину инцидентов посредством анализа вредоносных действий или объектов, обнаруженных с помощью индикаторов атаки. Это доказывает высокую эффективность такого подхода к обнаружению продвинутых атак и сложных угроз без применения вредоносного ПО. Однако чем точнее вредоносная активность имитирует нормальное поведение пользователей и администраторов, тем больше число потенциальных ложноположительных срабатываний, а значит, снижается информативность оповещений. Эту проблему тоже нужно решать.

На нейтрализацию без очереди

Опытные злоумышленники зачастую используют те же инструменты на тех же рабочих местах и обращаются к тем же системам с теми же временными интервалами, что и настоящие системные администраторы, – их действия ничем не выделяются. В этом случае окончательное решение может принять только аналитик. Он решит, является ли наблюдаемая активность вредоносной или легитимной. В конце концов, он может просто спросить конкретного сотрудника, выполнял ли тот те или иные действия.

Однако аналитики SOC могут работать лишь с ограниченным объемом информации. Поскольку на основе экспертной проверки и приоритизации автоматических обнаружений принимается решение о дальнейшем расследовании и реагировании, очень важно как можно скорее определить, является ли наблюдаемое поведение нормальным для конкретной IT-инфраструктуры. Наличие базового представления о нормальной активности помогает сократить количество ложноположительных срабатываний и повысить эффективность обнаружения угроз.

При большом числе ложноположительных срабатываний и интенсивном потоке оповещений, требующих проверки и расследования, среднее время реагирования на реальные инциденты может существенно вырасти. Здесь-то и приходит на помощь машинное обучение. Модели машинного обучения можно натренировать на оповещениях, уже проверенных и классифицированных аналитиками SOC. Присваивая оповещениям определенные рейтинги, модель машинного обучения может значительно облегчить приоритизацию, фильтрацию, создание очередей событий и т. д. Проприетарная модель машинного обучения «Лаборатории Касперского» позволяет автоматизировать процесс первоначальной приоритизации инцидентов и минимизировать среднее время реагирования за счет повышения производительности аналитиков.

Качественное расследование базируется на качественных данных

Злоумышленники атакуют один хост за другим, поэтому необходимо соотносить оповещения, поступающие с защищенных активов. Для создания эффективной стратегии реагирования важно выявить все затронутые хосты и получить полную картину их активности. В некоторых случаях может потребоваться дополнительное расследование. Аналитики собирают как можно больше контекстной информации, чтобы определить уровень опасности инцидента. Он зависит от нескольких факторов, в частности от того, кто стоит за атакой, на каком этапе она была обнаружена (какова цепочка поражения), сколько активов было затронуто и какие, что еще характеризует угрозу и как она связана с конкретной компанией, каков ущерб инфраструктуре, насколько сложным будет восстановление и т. д. Для понимания происходящего нужен доступ к постоянно обновляемой информации о злоумышленниках, их мотивации, используемых методах и инструментах и потенциальном ущербе, который они могут нанести. Сбор таких сведений требует много времени и высокой квалификации.

SOC «Лаборатории Касперского» анализирует полученные данные с использованием всех имеющихся у нас знаний о тактиках, методах и процедурах киберпреступников по всему миру (рис. 3). Наши источники – результаты исследований угроз, база знаний MITRE ATT&CK, десятки ежегодных проверок защищенности во всех отраслях, непрерывный мониторинг безопасности и опыт реагирования на инциденты. Эти постоянно дополняемые сведения помогают обнаруживать маскирующиеся угрозы, не использующие вредоносное ПО, и формировать полную картину ситуации. Так мы можем эффективнее расследовать пограничные случаи и предоставлять клиентам четкие инструкции по реагированию.

Рис. 3. Процесс анализа инцидентов в Kaspersky Managed Detection and Response

Время действовать

Стратегия реагирования выработана – пора переходить к действиям. И, как правило, сервисы MDR на этом заканчиваются. Клиенты получают отчеты об инцидентах с конкретными рекомендациями, и предполагается, что дальше они реализуют эти меры своими силами. Однако учитывая, что клиент выбрал сервис MDR в первую очередь из-за нехватки ИБ-специалистов, а рекомендации часто содержат узкоспециальную информацию и могут быть не вполне понятны, своевременное и эффективное реагирование оказывается под вопросом. Отсутствие средств централизованного автоматического реагирования усугубляет проблему и сводит на нет пользу сервиса.

Kaspersky Managed Detection and Response использует передовые технологии безопасности на основе аналитических данных об угрозах и машинного обучения. Сервис автоматически предотвращает большинство угроз, проверяя при этом все оповещения продуктов, и проактивно анализирует метаданные активности системы на наличие признаков активной или готовящейся атаки. Kaspersky Managed Detection and Response задействует тот же агент, что и Kaspersky Endpoint Detection and Response и Kaspersky Sandbox, но открывает дополнительные возможности после активации. Агент позволяет изолировать зараженные хосты, завершать несанкционированные процессы, помещать на карантин и удалять вредоносные файлы, и все это – удаленно, в один клик.

Kaspersky MDR подстраивается под требования вашей организации и может предложить полностью управляемую защиту от угроз или реагирование на основе подготовленных экспертами инструкций. При этом все меры реагирования будут под вашим контролем. Рекомендации по реагированию на инциденты написаны простым и понятным языком – вы можете сразу переходить к действиям. Пользователи Kaspersky Managed Detection and Response могут использовать агент EDR, чтобы принимать рекомендованные меры реагирования самостоятельно, или заранее предоставить «Лаборатории Касперского» право удаленно осуществлять автоматическое реагирование для тех или иных типов инцидентов.

Выводы

Ни автоматизированное обнаружение, ни активный поиск угроз сами по себе не являются панацеей от многочисленных современных атак. Однако сочетание традиционных средств обнаружения и предотвращения угроз до компрометации с последующим итеративным поиском новых угроз, пропущенных автоматизированными инструментами, может быть очень эффективным. Kaspersky Managed Detection and Response позволяет извлечь максимум из используемых вами защитных решений «Лаборатории Касперского», предоставляя полностью управляемые, индивидуально настраиваемые возможности обнаружения, приоритизации, расследования и реагирования.

Противодействие целевым атакам требует большого опыта и постоянного обучения. Около десяти лет назад «Лаборатория Касперского» стала одной из первых компаний, организовавшей специализированный центр для расследования сложных угроз, и обнаружила больше крупномасштабных целевых атак, чем другие поставщики. Благодаря нашему уникальному опыту вы можете пользоваться ключевыми преимуществами Security Operation Center – без затрат на его создание.

Новости о киберугрозах: www.securelist.ru
Новости IT-безопасности: business.kaspersky.ru

www.kaspersky.ru

kaspersky **АКТИВИРУЙ БУДУЩЕЕ**