KASPERSKY lab

Передовая защита от сложных угроз и снижение риска целевых атак

Kaspersky Anti Targeted Attack Platform

www.kaspersky.ru
#ИстиннаяБезопасность

Передовые угрозы и целевые атаки – опаснее с каждым годом

По статистике, в 2016 году затраты на ликвидацию инцидента целевой атаки увеличивались в среднем на 200%, если компании-цели начинали восстановительные работы через неделю и больше после начала атаки.

* Результаты глобального исследования рисков корпоративной IT-безопасности за 2016 г., проведенного «Лабораторией Касперского».

Любая крупная компания, занимающая значительный сегмент своего рынка, – потенциальная цель атак. Однако это не означает, что небольшие предприятия в безопасности: часто преступники видят в них легкую промежуточную цель на пути к крупной добыче. А для лидеров рынка вероятность стать жертвой такой атаки возрастает еще больше. Атака — лишь вопрос времени.

Ландшафт угроз

В настоящее время наибольшую опасность для корпоративных систем пердставляют целевые атаки и сложные угрозы, включая комплексные таргетированные угрозы (APT). Усугубляет эту ситуацию еще и то обстоятельство, что огромное количество организаций пытаются защититься от новейших угроз при помощи устаревших технологий безопасности, в то время как киберпреступники постоянно совершенствуют свои методы.

Целевые атаки могут длиться неделями, месяцами и даже годами, оставаясь незамеченными, и все это время их организатор будет собирать информацию и находить новые способы использовать уникальные уязвимости в системе жертвы. В отличие от обычного вредоносного ПО, целевые атаки осуществляются под активным контролем и управлением злоумышленника. Преступники стремятся закрепиться внутри корпоративного периметра и получить незаметный и зачастую полный контроль над системами. Организаторы таких атак терпеливо и часто очень тщательно исследуют жертву и готовы ждать, пока их старания не будут щедро вознаграждены.

Средние затраты в результате одной целевой атаки:

Кто организует атаки?

Киберпреступники – продают данные тому, кто больше заплатит, или просто похищают деньги. Обычно создают инструменты для преступления сами или покупают их в «подпольном» интернете.

Конкурирующие компании – ищут конфиденциальные данные или даже пытаются совершить саботаж. Обычно оплачивают «услуги» наемных исполнителей.

Наемные исполнители – профессионалы кибершпионажа; разрабатывают собственные инструменты и продают свои «услуги» тому, кто больше заплатит.

Хактивисты – заявляют, что имеют благие цели, изобретательны, используют сложный инструментарий и составляют серьезную проблему для любой организации, привлекшей их внимание.

Правительственные органы – правительства во всем мире ведут регулярную слежку за отдельными лицами, группами и компаниями, хотя и отрицают это. Их инструментарий может быть чрезвычайно изощренным, дорогостоящим и сложным для обнаружения.

Внутренние и внешние факторы, способствующие успешной атаке

Успеху злоумышленников, ведущих целевые атаки против IT-инфраструктур, способствует ряд ключевых факторов, включая следующие:

- отсутствие профилактики и завышенная оценка возможностей имеющейся защиты;
- недостаточная осведомленность сотрудников о рисках информационной безопасности;
- непрозрачность IT-среды и в особенности сетевой маршрутизации;
- собственное и устаревшее ПО и операционные системы;
- отсутствие у специалистов по безопасности знаний в области исследования вредоносных программ, цифровой криминалистики, реагирования на инциденты и аналитики угроз.

В чем состоит риск?

Риски для всех организаций:

- несанкционированные транзакции
- кража или повреждение критически важных для бизнеса данных
- незаметная манипуляция процессами
- подрывная деятельность конкурентов
- шантаж и вымогательство
- кража персональных данных

Риски для ключевых отраслей:

Финансовые услуги

- несанкционированные транзакции
- атаки на банкоматы с похищением наличности
- кража персональных данных

Государственные услуги

- манипуляция данными
- шпионаж
- ограниченная доступность онлайн-услуг
- кража персональных данных
- действия хактивистов

Производство и высокие технологии

- шпионаж (производственные секреты)
- компрометация критически важных технологических процессов

Телекоммуникации

- атаки на корпоративных клиентов посредством телекоммуникационной инфраструктуры
- манипуляция почтовыми серверами как средство социальной инженерии
- контроль выставления счетов
- манипуляция веб-ресурсами как средство фишинга
- использование скомпрометированной инфраструктуры (устройств/интернета вещей) для DDoS-атак

Энергоснабжение и коммунальные услуги

- манипуляции результатами расчетов
- атаки на технологические сети с нанесением физического ущерба

СМИ

- хактивизм
- компрометация веб-сайтов (взлом, фишинг)
- распространение атак на широкую аудиторию

Здравоохранение

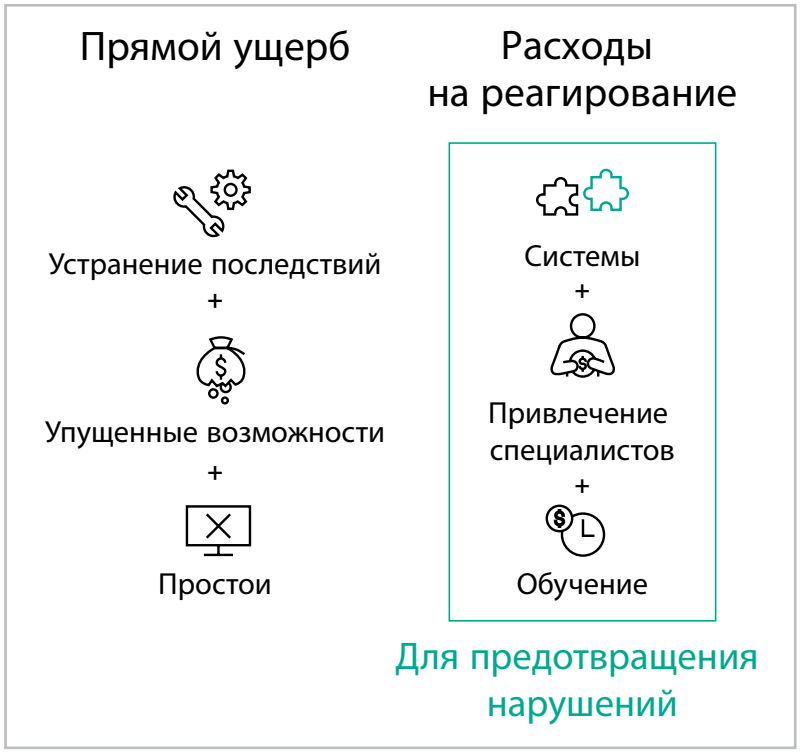
- похищение информации о пациентах
- атаки на оборудование для дистанционного оказания медицинских услуг

Целевые атаки: киберпреступность как бизнес

Большинством целевых атак руководят опытные хакеры и киберпреступники. Они адаптируют атаки на каждом этапе так, чтобы обойти традиционные средства защиты, использовать уязвимости и похитить как можно больше ценностей, будь то деньги, конфиденциальная информация или другие ресурсы.

За целевыми атаками стоят профессионалы, для которых киберпреступления – способ заработка. Выбирая и атакуя предприятие, они руководствуются единственной целью: получить максимальную прибыль. Ее они рассчитывают еще до атаки, учитывая сопутствующие расходы и потенциальное «вознаграждение». Разумеется, злоумышленники стремятся минимизировать начальные затраты, используя наиболее дешевые средства атаки и добиваясь максимальной финансовой отдачи.

Для большинства целевых атак применяется сочетание социальной инженерии и специально подобранного набора инструментов, часто разработанного для конкретной атаки. В наши дни стоимость запуска эффективной целевой атаки значительно снизилась, и соответственно возросло общее количество атак в мире.



Что же стоит на кону, когда организация подвергается целевой атаке?

Прямые финансовые убытки. Злоумышленники могут попытаться похитить данные для доступа к корпоративным банковским счетам, чтобы провести неправомерные транзакции.

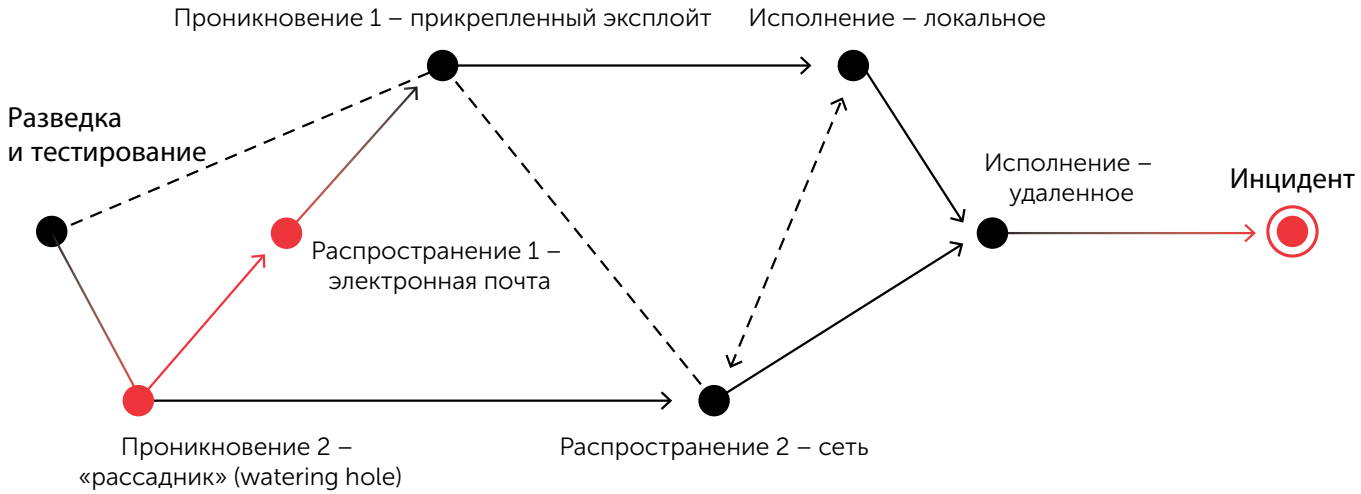
Нарушение важнейших бизнес-процессов. Блокировка или замедление критически важных бизнес-процессов могут быть лишь побочными эффектами некоторых атак, однако существуют и атаки, разработанные специально для саботажа. Даже после обнаружения подобной атаки бизнес-процессы возобновляются не сразу: организации нужно время, чтобы провести расследование и заново наладить работу. Такой простой может привести к потере потенциальных клиентов.

Расходы на восстановление. В случае обнаружения целевой атаки, компания стакливается с целым рядом затрат, которые не были заложены в бюджет. Восстановление систем и процессов может потребовать и капитальных и операционных затрат, например на привлечение консультантов по безопасности и настройке систем.

Анатомия целевой атаки

Теоретически цепочка поражения в результате целевой атаки достаточно проста: разведка и тестирование; проникновение; распространение; исполнение; результат. Казалось бы, автоматическое блокирование первых шагов такой многоступенчатой атаки должно ее остановить.

Однако в действительности целевые атаки крайне сложны, а алгоритм их развития и исполнения нелинеен. Поэтому стратегия защиты должна насчитывать множество уровней, включая и автоматическое обнаружение, и постоянный мониторинг, и активный поиск угроз.



Для некоторых атак используется метод комплексных таргетированных угроз (APT) – они могут быть очень эффективными, но обходятся недешево, – а для других применяются более простые методы, например комплексное вредоносное ПО или уязвимости «нулевого дня».

Целевая атака – это длительный процесс, который нарушает безопасность и позволяет киберпреступнику несанкционированно управлять IT-инфраструктурой жертвы, избегая обнаружения традиционными средствами защиты.

Атака этого типа – целый проект, а не отдельное вредоносное действие. Опыт отслеживания глобальных угроз показывает, что такие операции часто длятся не менее 100 дней, а атаки на правительственные учреждения, крупных игроков рынка и критически важные инфраструктуры могут вестись годами.

Кроме того, этот процесс направлен на конкретную инфраструктуру, призван преодолеть конкретные механизмы безопасности и часто начинается с воздействия на выбранных сотрудников через электронную почту или социальные сети. Этот подход кардинально отличается от используемого злоумышленниками, распространяющими обычные вредоносные программы путем массовой рассылки, – они преследуют совершенно другие цели. В случае с целевой атакой методы и этапы цепочки поражения подбираются для конкретной жертвы.

Процессом целенаправленной атаки обычно управляет организованная группа или команда профессионалов (иногда международная), вооруженная сложными техническими средствами. Можно даже сказать, что их деятельность – это не просто проект, а целая «военная операция». Например, атакующие часто составляют список сотрудников, которые могут «впустить» их в сеть целевой организации, а затем изучают их профили в интернете и действия в соцсетях. После заражения рабочего места такого сотрудника злоумышленники проникают в сеть, контролируя которую они могут направлять вредоносные действия так, как им нужно.

Коротко о «песочницах»

Многие так называемые решения для обнаружения целевых атак, предлагаемые на рынке, представляют собой просто «песочницы». «Песочницы» появились даже у тех поставщиков, у которых нет опыта в обнаружении новых комплексных угроз; такие решения обычно являются лишь дополнением к антивирусному ядру и не опираются на масштабные аналитические данные об угрозах.

Передовая «песочница» «Лаборатории Касперского» – это один из многочисленных уровней детектирования угроз, используемых в решении Kaspersky Anti Targeted Attack Platform. Она создана непосредственно на основе нашего внутреннего комплекса «песочниц», который мы используем уже более десяти лет. Эта технология усовершенствована на основе статистики, собранной за десять лет анализа угроз. Она гораздо лучше приспособлена к борьбе с целевыми атаками, нежели «песочницы» многих других компаний, предлагаемые ими как панацея.

Проблемы защиты корпоративных инфраструктур

По мере того как риск сложных угроз растет по экспоненте, многие предприятия подходят к вопросу своей безопасности без разностороннего подхода и стратегического планирования и просто внедряют новые технологии и сервисы, надеясь достигнуть большей прозрачности и лучшей защиты от развивающихся угроз. Однако эти усилия могут не оправдать себя.

Фрагментарное и непоследовательное укрепление защиты приносит весьма скромные результаты по нескольким причинам:

1. **Отдача от инвестиций в «песочницу», в отдельные технологии или в организацию центра обеспечения безопасности (SOC) несопоставима с затратами.**

   Средства защиты периметра, такие как сетевые экраны и решения для защиты от вредоносного ПО, способны противостоять случайным, непродуманным атакам. В случае с целевыми атаками дело обстоит иначе.

   Некоторые поставщики защитных решений пытаются решить проблему APT, используя ряд отдельных, разрозненных продуктов: «песочниц», средств анализа аномалий в сети и даже мониторинга, направленного на рабочие места. Эти обособленные компоненты обеспечивают некоторую защиту и до известных пределов блокируют средства киберпреступников, но самих по себе их недостаточно для обнаружения скоординированной целевой атаки: здесь необходима способность выявлять множество событий на всех уровнях корпоративной инфраструктуры.

   Собранная информация должна обрабатываться системой многоуровневого анализа. Затем ее нужно интерпретировать при помощи аналитических данных, поступающих из надежного источника в режиме реального времени. Другими словами, наибольшего успеха позволяет достичь подход, при котором используется целый ряд связанных между собой передовых технологий (в том числе «песочница» с анализом аномалий в сети и анализом событий на рабочих местах), интегрированных в общий, комплексный процесс.

2. **Имеющиеся решения создают слишком много разрозненных событий безопасности**, которые SOC не успевает обрабатывать, анализировать, сортировать и разрешать в приемлемый срок.

3. **Отсутствуют навыки в области реагирования, соответствующие текущему уровню сложности атак.** Специалисты по безопасности могут умело обнаруживать атаки и быстро устранять их последствия (использовать «золотые образы», добавлять URL-адреса и файлы в черные списки, создавать политики), но при этом не обладать всеми нужными навыками для полного цикла реагирования (оценивать уровень риска, проводить начальный и криминалистический анализ, расследовать инциденты и блокировать распространение вредоносных файлов).

4. **Следы атаки тщательно скрываются.** В ходе целевой атаки преступники могут без труда обойти традиционные защитные решения, используя похищенные учетные данные и легитимное ПО, и не нарушая явным образом безопасность системы.

   Поскольку злоумышленники прилагают все усилия, чтобы скрыть свои вредоносные действия, штатному отделу IT-безопасности иногда непросто заметить атаку – а это значит, что она может продолжаться в течение продолжительного времени.

   Проблема заключается в том, что только 40% нарушений безопасности вызвано действием вредоносного ПО: как сказано выше, атакующие используют целый ряд методов, чтобы получить доступ к корпоративным системам.

   Даже если вредоносное ПО и применяется, в 70–90% случаев оно создано специально для организации-жертвы (Verizon: «Отчет о расследованиях взломов» (Data Breach Investigation Report)).

5. **Трудно решить, с какими задачами обеспечения защиты способны справиться автоматизированные системы, для каких нужно нанимать и обучать внутренних сотрудников, а для каких нужно привлекать внешних консультантов.**

   С ростом серьезности инцидентов безопасности и их потенциального влияния на общую эффективность бизнеса одной из главных проблем для компаний становится поиск экспертов нужной квалификации. Для наибольшей эффективности стратегия безопасности должна включать не только постоянный мониторинг и обнаружение, но и возможности быстрого реагирования и квалифицированного устранения последствий, а также процессы криминалистического анализа.

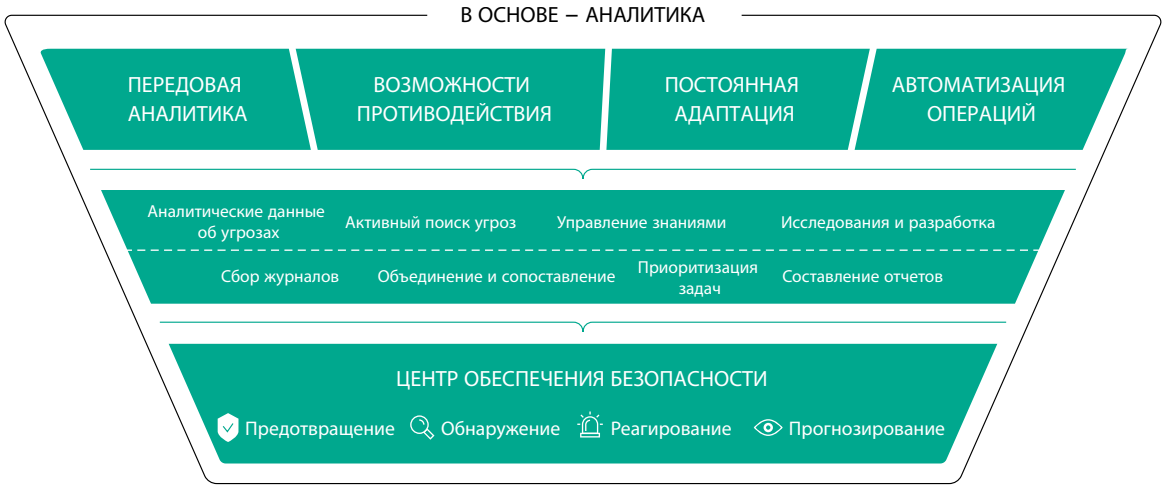
Обычно SOC направляют усилия только на часть задач по обнаружению и реагированию.. Применение автоматизированных решений позволяет освободить специалистов для выполнения последующих этапов процесса управления инцидентами, но мало какие предприятия могут выполнять каждую задачу высокого уровня своими силами. Поэтому требуется определить, за какие компоненты общего процесса (управление, оценка уровня риска, приоритизация, быстрое восстановление) должны отвечать внутренние сотрудники, а какие (исследование вредоносных программ, цифровая криминалистика, реагирование на инциденты, активный поиск угроз) лучше передать внешним специалистам.

Значимость аналитики для SOC

Адаптируя свои методы, киберпреступники обходят привычные средства защиты и незаметно действуют в пораженной инфраструктуре. Корпоративные системы безопасности также должны адаптироваться, используя многоуровневую защиту IT-инфраструктуры на основе аналитических данных.

До недавнего времени безопасность периметра корпоративной сети обеспечивали широко доступные защитные технологии, которые предотвращали заражение вредоносным ПО или несанкционированный доступ в корпоративную сеть. Однако сегодня, когда резко растет число целевых атак, столь простой подход к обеспечению безопасности потерял эффективность.

Для успешной борьбы с новыми угрозами отдел ИБ должен применять современный подход, при котором традиционный SOC вооружен аналитическими данными об угрозах и решениями, обеспечивающими многоуровневую безопасность.



Улучшение процессов корпоративной безопасности

Отдел информационной безопасности отвечает за организационную и техническую защиту критически важной информации и бизнес-процессов в сложных IT-средах. В таких средах, например, все чаще внедряются автоматизированные решения и программные компоненты, а также происходит переход на электронный документооборот.

Лавинообразный рост объема комплексных угроз и целевых атак привел к росту количества используемых решений. Для того чтобы собирать, сохранять и обрабатывать созданные неструктурированные данные, а также обнаруживать и приоритизировать сложные многоуровневые атаки, нужно обновлять существующие процессы:

- приоритизация угроз вручную и оценка факторов, которые могут указывать на выполнение целевой атаки;
- сбор информации о целевых атаках и статистики комплексных угроз;
- обнаружение инцидентов и реагирование на них;
- анализ подозрительных объектов в сетевом трафике и вложениях электронной почты;
- обнаружение аномальной активности в защищаемой инфраструктуре.

Крупные предприятия отвечают на современные комплексные угрозы, переходя на централизованное управление информационной безопасностью, консолидируя данные разнородных защитных решений (путем автоматизации сбора данных и сопоставления событий в системах SIEM) и обеспечивая их единое представление посредством создания центров обеспечения безопасности (SOC). Однако для того, чтобы эффективно бороться с целевыми атаками и комплексными угрозами, требуется полное понимание проблем безопасности и глубокие знания в области анализа киберугроз.

Решение

В 2008 году «Лаборатория Касперского» стала первой IT-компанией, создавшей специальный центр для исследования комплексных угроз.

Именно благодаря этому «Лаборатория Касперского» обнаружила больше комплексных целевых угроз, нежели любой другой поставщик защитных решений. Когда вы узнаете из новостей об очередной целевой атаке, высока вероятность, что ее обнаружило особое подразделение «Лаборатории Касперского» – глобальный центр исследования и анализа угроз (GReAT).

GReAT сыграл важную роль в обнаружении многих целевых атак, в том числе:

- Stuxnet
- RedOctober
- Flame
- Miniduke
- Epic Turla
- DarkHotel
- Duqu
- Carbanak
- Equation

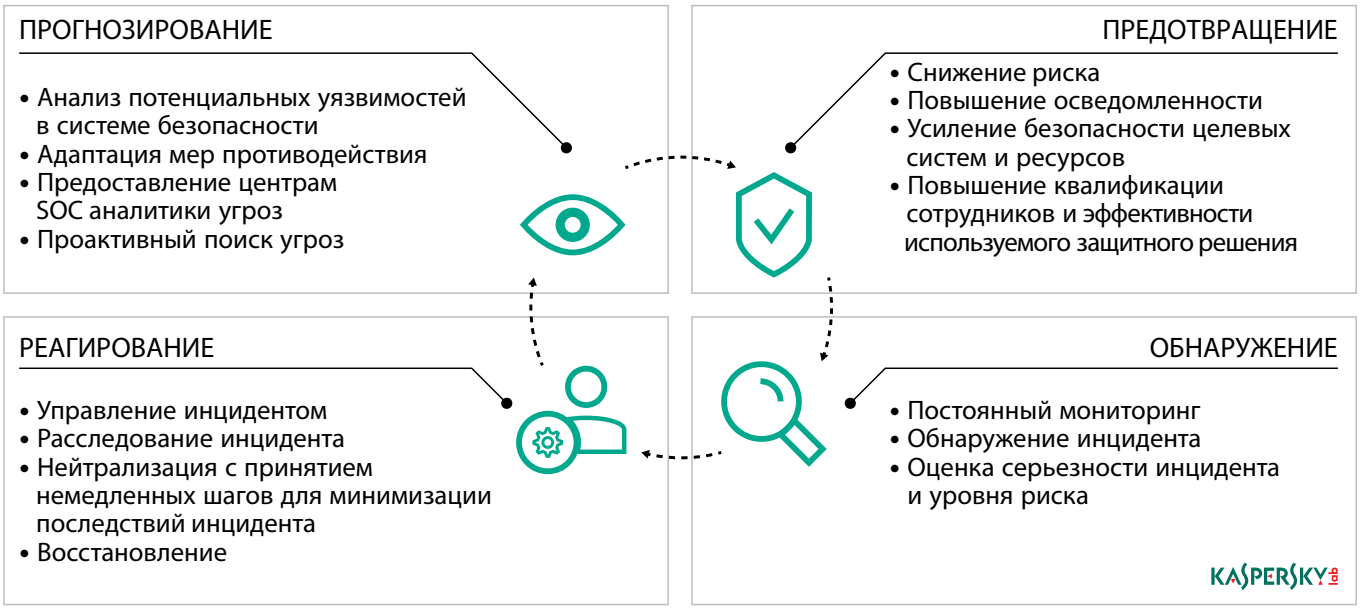
...и целого ряда других.

Понимая принципы работы сложнейших в мире угроз, «Лаборатория Касперского» создала набор технологий и сервисов, позволяющий реализовать адаптивный подход к защите от целевых атак. Благодаря опыту и знаниям экспертов, машинному обучению и обработке больших данных об угрозах «Лаборатория Касперского» занимает первые места в независимых тестах чаще, чем какой-либо другой поставщик решений безопасности[1]. Мы готовы передать этот опыт и инструменты обнаружения целевых атак нашим заказчикам в виде отдельного решения – результата двадцатилетней работы по выявлению и анализу угроз, положенной в основу созданных технологий.

Большинство простых киберугроз блокируются традиционными технологиями обеспечения безопасности, работающими на основе сигнатур и/или элементов эвристического анализа, однако сегодня хакеры и киберпреступники проводят все более сложные атаки, нацеленные на конкретные организации. Современные целевые атаки, в том числе APT-класса, представляют собой одну из наибольших опасностей для предприятий. В то время как угрозы – и приемы, которыми пользуются хакеры и киберпреступники, – развиваются, многие организации не адаптируют к ним собственную стратегию обеспечения безопасности.

Целевые атаки и комплексные угрозы становится все труднее обнаруживать и зачастую еще труднее устранять, поэтому для борьбы с ними требуется комплексная и гибкая стратегия. В основе адаптивной стратегии обеспечения безопасности, предлагаемой «Лабораторией Касперского», лежит наиболее перспективная (по мнению Gartner) защитная архитектура. Наш подход предполагает циклическое выполнение действий в четырех основных областях: предотвращение, обнаружение, реагирование и прогнозирование.

- Предотвращение – снижение риска комплексных целевых атак.
- Обнаружение – выявление действий, которые могут свидетельствовать о ведении целевой атаки.
- Реагирование – устранение брешей в системе безопасности и расследование атак.
- Прогнозирование – предположение о том, где и когда ожидать новых целевых атак.



В основе такого подхода лежит понимание того, что традиционные системы предотвращения угроз должны функционировать взаимодействуя с технологиями обнаружения и анализа угроз, возможностями реагирования и методами профилактической защиты. Это позволяет создать систему кибербезопасности, которая постоянно адаптируется и отвечает на возникающие угрозы для предприятий.

1 Подробнее: Kaspersky.ru/top3

Обнаружение при помощи многовекторных технологий

В случае с целевыми атаками важно, чтобы технологии предотвращения отсеивали инциденты, связанные с общим вредоносным ПО, обычными «простыми» угрозами, нерелевантными коммуникациями.

Для того чтобы снизить привлекательность вашей компании как объекта атаки, необходимо заниматься комплексным усилением системы безопасности (при помощи специальных решений), а также обучением сотрудников в области информационной безопасности, в том числе повышением осведомленности о возможных угрозах и атаках.

80% целевых атак начинаются с отправки вредоносного сообщения электронной почты, содержащего вложение или ссылку.

Киберпреступники предпочитают проникать в систему через части организаций, которые считаются наименее подготовленными к противодействию угрозам. Часто таковыми являются отделы кадров, справочные центры, личные помощники старших руководителей, а также зоны ответственности компании, отданные внешним специалистам.

Традиционные защитные технологии, ориентированные на предотвращение, могут выявить некоторые инциденты, происходящие в ходе целевой атаки, но, как правило, не определяют, что такие отдельные инциденты являются частью куда более сложной и опасной угрозы, которая уже наносит серьезный ущерб вашему бизнесу – и будет делать это еще долго.

Однако такие технологии предотвращения сохраняют свое значение как ключевой элемент нового, проактивного подхода к защите от целевых атак.

Предприятиям важно продолжать использовать традиционные технологии безопасности:

1. для автоматизации фильтрации и блокирования событий и инцидентов, не связанных с целевыми атаками, – это позволяет сосредоточить все внимание на обнаружении инцидентов, действительно указывающих на такие угрозы;

2. для усиления защиты IT-инфраструктуры от атак, задействующих дешевые и простые в применении средства (социальную инженерию, съемные и мобильные устройства, вредоносные программы, зараженные сообщения электронной почты и т. д.). В сущности, все уже сделанные вложения в защиту периметра и рабочих мест, а также внедренные средства контроля усложняют киберпреступникам проникновение в вашу сеть.

Но если мотивация атакующего достаточно высока или он нанят третьей стороной, которая требует успешного выполнения «задания», одного предотвращения будет недостаточно.

Угрозы различных типов и соответствующие технологии безопасности

Обнаружение атаки – до того, как она нанесет ущерб

В состав решения Kaspersky Anti Targeted Attack Platform входят:

- Сенсоры, объединенные в многоуровневую структуру. Благодаря сочетанию сетевых сенсоров, веб-сенсоров, почтовых сенсоров, сенсоров рабочих мест, решение KATA обеспечивает полную прозрачность (расширенный мониторинг и обнаружение возможных атак) на каждом уровне корпоративной IT-инфраструктуры.
- Передовая «песочница». Созданная в результате непрерывного процесса разработки, длившегося свыше десяти лет, изолированная виртуальная среда для безопасного исполнения подозрительных объектов, позволяющая наблюдать за их поведением и оценивать новые угрозы.
- Мощные аналитические технологии. Быстро генерирующие вердикты с нулевым числом ложных срабатываний.
- Анализатор целевых атак. Созданный «Лабораторией Касперского» и позволяющий оценивать данные, поступающие с сетевых сенсоров и сенсоров рабочих мест, и быстро создающий вердикты по обнаружению угроз для отдела ИБ.

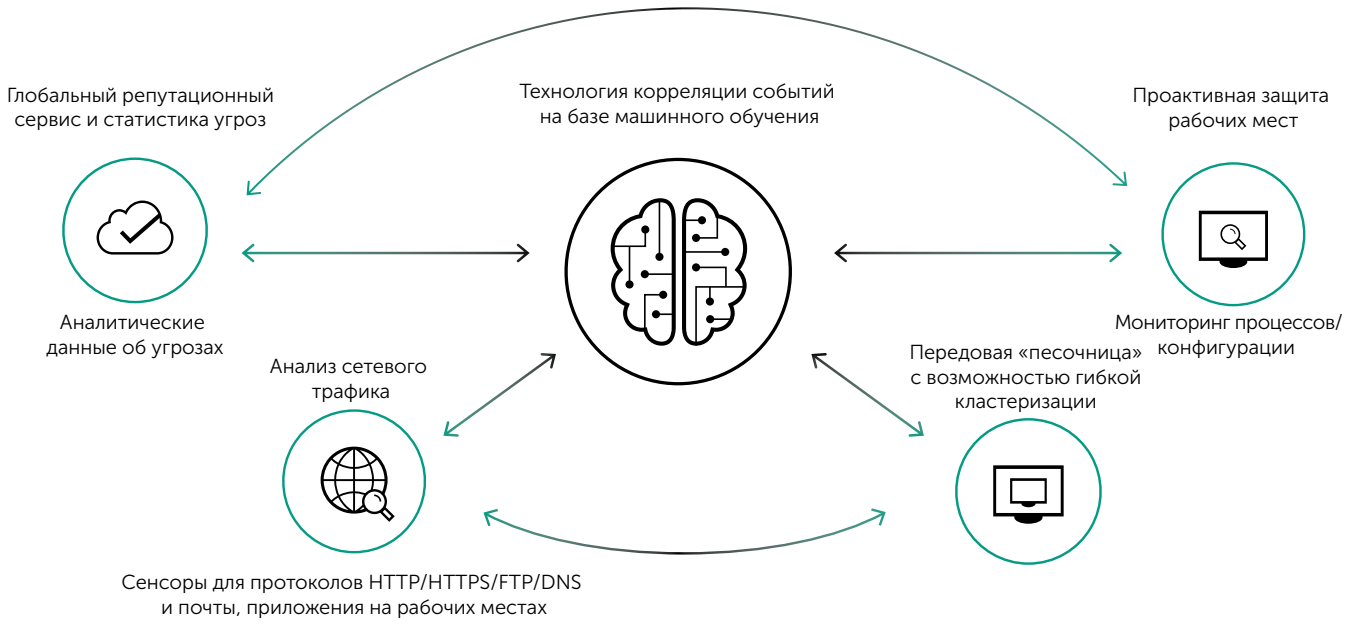
Чем раньше обнаружена целевая атака, тем меньшие убытки несет организация и тем меньше нарушаются ее процессы. Именно поэтому качество и эффективность обнаружения особенно важны.

Способность обнаруживать целевые атаки достигается объединением решений и сервисов, обеспечивающих следующее:

- обучение;
- применение опыта в обнаружении целевых атак – выполнение разового аудита инфраструктуры для поиска следов компрометации;
- использование специализированного решения – Kaspersky Anti Targeted Attack Platform;
- доступ к потокам данных об угрозах для обмена информацией и получения обновлений о новых угрозах в режиме реального времени;
- возможность создания настраиваемых отчетов и отчетов об APT, позволяющих лучше понять источники и методы атак.

Kaspersky Anti Targeted Attack Platform (KATA) – это инновационное решение, возможности которого по обнаружению атак намного превосходят традиционные технологии для предотвращения угроз.

KATA – часть адаптивного, интегрированного подхода к корпоративной безопасности. Мониторинг сетевого трафика в режиме реального времени в сочетании с анализом поведения подозрительных объектов в песочнице и проактивной защитой рабочих мест дает подробную картину того, что происходит в масштабах корпоративной IT-инфраструктуры. Сопоставляя события на разных уровнях (включая сеть, рабочие места и глобальную среду), KATA обнаруживает комплексные угрозы практически в режиме реального времени и облегчает расследование произошедших инцидентов.

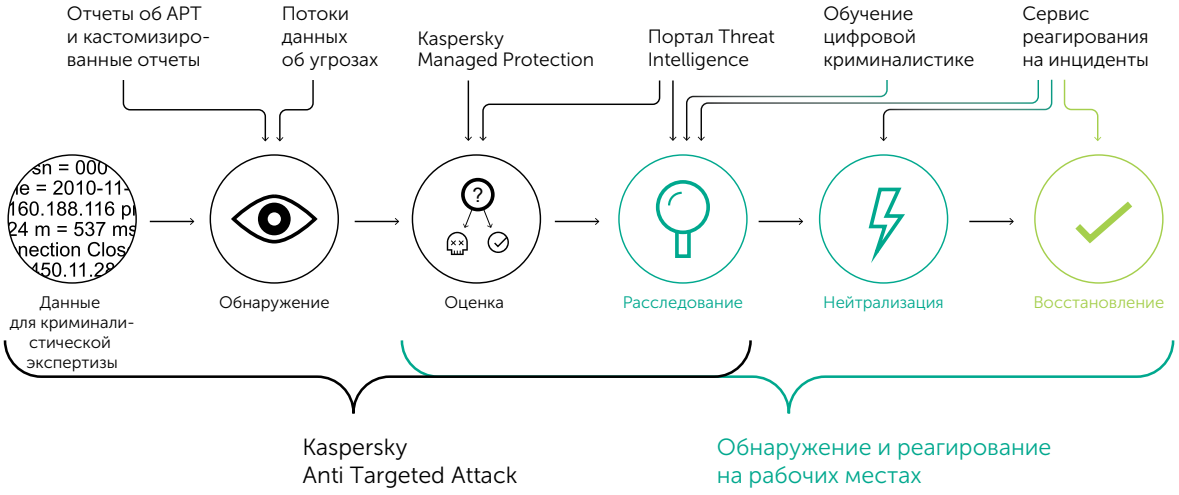


Реагирование – быстрое восстановление после атак

Высокий процент обнаружения угроз – это еще не окончательная победа. Даже самые лучшие технологии обнаружения мало помогут в защите вашей организации без инструментов и знаний, позволяющих быстро отреагировать на уже активную угрозу.

Важно, чтобы на случай обнаружения атаки была возможность обратиться к признанным экспертам по безопасности, которые обладают необходимыми навыками и опытом и способны:

- быстро восстановить операции;
- получить аналитические данные по результатам расследования инцидента, на основе которых можно действовать;
- спланировать действия для предотвращения повторных атак по такому же сценарию.
- оценить ущерб и исправить ситуацию.



Эксперты «Лаборатории Касперского» могут помочь в анализе целевой атаки. Наш сервис реагирования на инциденты включает следующие услуги:

- **Оценка инцидента.** Первоначальный анализ инцидента, который проводится предельно быстро (дистанционно или с выездом на место), чтобы снизить ущерб для бизнеса.
- **Сбор улик.** Например, сбор образов жестких дисков, дампов памяти, трассировок сети и другой информации, относящейся к инциденту.
- **Криминалистический анализ.** Тщательный анализ, помогающий понять:
  - какие системы подверглись атаке;
  - кто проводил атаку;
  - в течение какого периода организация подвергалась атаке;
  - откуда началась атака;
  - почему была атакована именно ваша организация;
  - как была реализована атака.
- **Анализ вредоносных программ.** Подробный анализ вредоносного ПО, использованного в рамках атаки.
- **План устранения последствий.** Подробный план, который поможет организации предотвратить дальнейшее распространение вредоносного ПО, а также спланировать удаление вредоносных программ и последствий их активности.
- **Отчет о расследовании.** Подробный отчет, содержащий информацию о расследовании инцидента и принятых мерах по устранению последствий.

Если ваша служба безопасности способна самостоятельно выполнить многие задачи по реагированию на инцидент, вы можете воспользоваться одним из следующих наших сервисов:

- **Сервис анализа вредоносного ПО** – тщательный анализ вредоносных программ, изолированных вашим отделом безопасности.
- **Сервис цифровой криминалистики** – анализ улик и последствий инцидента, собранных вашим отделом безопасности.

Прогнозирование – проактивная защита от будущих угроз

Ландшафт угроз постоянно меняется, и ваша стратегия безопасности должна постоянно развиваться, чтобы отвечать на новые вызовы.

Обеспечение безопасности – это не разовое мероприятие, а постоянный процесс, который предусматривает регулярную оценку:

- последних угроз;
- эффективности системы IT-безопасности.

Это позволит вашей компании адаптироваться к новым рискам и меняющимся требованиям.

Доступ к экспертам, которые знают о последних изменениях глобального ландшафта угроз, а также помогут протестировать ваши системы и имеющиеся защитные технологии, – важнейшее условие адаптации вашей организации к новейшим угрозам.

За многие годы работы эксперты «Лаборатории Касперского» накопили огромный объем знаний о принципах работы комплексных и целевых атак – и продолжают постоянно наращивать эти знания, анализируя новые приемы злоумышленников. Опыт, ставший результатом огромной работы, позволяет прогнозировать появление новых методов атак и помогать в подготовке к борьбе с такими атаками.

Приняв адаптивную стратегию обеспечения безопасности, предлагаемую «Лабораторией Касперского», вы добьетесь следующего:

1. Вы перейдете с реактивной на проактивную модель безопасности, основанную на управлении рисками, постоянном мониторинге, обоснованном реагировании на инциденты и активном поиске угроз.

2. Структура ваших операций будет способствовать выполнению повседневных процессов защиты и повышать ее эффективность за счет многоуровневой защитной модели, предотвращающей и выявляющей комплексные атаки на каждом этапе их развития.

3. Благодаря единой интегрированной платформе сократится число оповещений о возможных угрозах, которые часто затрудняют работу отдела IT-безопасности, если их слишком много: для сокращения числа оповещений используются контекст, полученный в ходе анализа угроз, и приоритизация возможных угроз, а также постоянное улучшение методов тактического реагирования за счет обмена знаниями об угрозах, обширного опыта и аналитических защитных сервисов.

4. Вы получите прозрачность и единое представление всех этапов атаки для аналитиков по безопасности, что позволяет без затруднений вести анализ атаки и уверенно расследовать действия известных и неизвестных угроз до того, как они нанесут ущерб бизнесу.

5. Вы будете заблаговременно получать уникальные знания о мотивах и намерениях киберпреступников благодаря обмену глобальной аналитикой угроз через портал аналитических данных об APT. Это позволит соответствующим образом приоритизировать политики и планируемые инвестиции в безопасность.

Кроме того, «Лаборатории Касперского» предлагает специализированные сервисы для укрепления защиты вашей IT-инфраструктуры:

- **Тестирование на проникновение.** Позволяет оценить эффективность используемых средств безопасности.
- **Анализ защищенности приложений.** Позволяет выявить уязвимости в программном обеспечении до того как это сделают киберпреступники.
- **Тренинги по кибербезопасности.** Помогают компании обучить собственных экспертов и организовать собственный центр обеспечения безопасности.
- **Аналитические отчеты и настраиваемые отчеты об угрозах.** Позволяют следить за постоянными изменениями ландшафта угроз.
- **Онлайн-сервис Threat Lookup.** Открывает доступ к глобальной базе данных об угрозах, которая вооружит вас нужными знаниями для исследования вредоносных программ.

Решение, доказавшее свою эффективность

Эффективность продуктов «Лаборатории Касперского» регулярно подтверждается результатами независимых тестирований. В 2016 году компания опередила всех производителей защитных решений по итогам независимых тестов. В 2016 г. «Лаборатория Касперского» приняла участие в 78 независимых тестированиях и обзорах. По результатам 70 тестов продукты компании оказались в тройке лучших, что соответствует показателю TOP-3 90%. В 55 тестах они заняли первое место. Это – весомое доказательство высочайшего качества защиты.

В апреле-мае 2017 года решение Kaspersky Anti Tageted Attack Platform успешно прошло тестирование, проводимое компанией ICSA Labs. Подобные испытания призваны проверить эффективность специализированных решений для защиты организаций от целевых атак.

Тестирование длилось 37 дней и включало 1104 теста: 585 атак и 519 проверок на ложные срабатывания. Упор в ходе исследования был сделан на новые и малоизвестные угрозы, которые позволяют предсказать, насколько успешно решение будет отражать атаки в реальных условиях.

По итогам тестирования Kaspersky Anti Tageted Attack Platform обнаружило 100% атак и не допустило ни одного ложного срабатывания. Таким образом, решение «Лаборатории Касперского» выполнило все условия для получения сертификата ICSA Labs Advanced Threat Defense (ATD).

Комплексный новаторский подход

Исследовательская компания Radicati Group в течение нескольких лет проводила независимый анализ рынка решений для защиты от APT, выявляя лидеров рынка (Top Players), новаторов (Trail Blazers), новых и нишевых специалистов (Specialists), а также зрелых игроков (Mature Players). По результатам опубликованного отчета об исследовании, подход «Лаборатории Касперского» к борьбе против целевых атак и комплексных угроз был признан инновационным и передовым.

В 2017 году решение KATA существенно улучшило свою позицию, перейдя из категории новых и нишевых игроков в категорию новаторов.

Новаторы применяют новые, передовые технологии, которые двигают вперед весь класс решений. Они не всегда располагают всеми возможностями и функциями (часто избыточными), которые требуются для попадания в категорию лидеров рынка. Тем не менее новаторы обладают потенциалом рыночного прорыва за счет уникальных технологий. Именно для этих игроков наиболее вероятен переход в категорию лидеров рынка.

www.kaspersky.ru

#ИстиннаяБезопасность

© 2017 АО «Лаборатория Касперского». Все права защищены. Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.