KASPERSKY lab

KASPERSKY ANTI TARGETED ATTACK PLATFORM

Стратегия противодействия целенаправленным атакам

www.kaspersky.ru

ЦЕЛЕНАПРАВЛЕННЫЕ АТАКИ И СЛОЖНЫЕ СОВРЕМЕННЫЕ УГРОЗЫ БЕЗОПАСНОСТИ

В самом начале своего развития целевые атаки требовали много интеллектуальных вложений и финансовых затрат, что сильно сужало круг потенциальных мишеней. В основном это были или государственные структуры, где в результате атак происходила утечка данных, или крупные банки, которые интересовали злоумышленников как места концентрации денежных средств. Сегодня распространение целевых атак затрагивает все новые секторы рынка (коммерческий, телекоммуникационный, промышленный и др.). Обусловлено это прежде всего существенным сокращением стоимости и трудозатрат при реализации самой атаки: большое количество ранее разработанных инструментов доступно хакерским группировкам, поэтому отсутствует острая необходимость создавать экзотические вредоносные программы с нуля. В большинстве своем современные целевые атаки построены на ранее созданных эксплойтах и вредоносном ПО, и лишь малая часть использует новые и уникальные технологии, которые преимущественно относятся к угрозам класса APT.

Прошло не так много времени с момента обнаружения одной из первых целевых атак Stuxnet в 2010 году, которая открыла миру глаза на новые по своим возможностям и своей эффективности методы проведения кибератак. Их высокая технологичность и использование уникального подхода для каждой из них затрудняют защиту инфраструктуры даже крупнейших компаний.

Участившиеся целевые атаки, в том числе с применением инструментов уровня APT, обостряют проблему обеспечения корпоративной кибербезопасности: потенциальные риски растут, что влечет за собой необходимость пересмотра существующей стратегии защиты организаций. Дело в том, что целевая атака совсем не похожа на типичные компьютерные угрозы или сетевые атаки, так как представляет собой набор целенаправленных действий, контролируемых злоумышленниками вручную на всех стадиях проникновения, что сильно выделяет ее в мире киберугроз.

АНАТОМИЯ ЦЕЛЕНАПРАВЛЕННОЙ АТАКИ

На подготовку целенаправленной атаки у злоумышленников могут уходить месяцы, а сама атака может оставаться незамеченной ещё дольше. Типичная целевая атака состоит из четырех этапов:

1) вначале проводится разведка и первичный сбор информации о компании-мишени, сотрудниках и партнерах, моделируется процесс проникновения и разрабатывается стратегия;

Для злоумышленников превентивная технология (даже с применением «песочницы») — это лишь ещё один уровень защиты, который нужно обойти. Обладая достаточным временем и знаниями, злоумышленник будет вбрасывать снова и снова «образцы», пока один из них не обойдет защиту. После этого проблема уже будет внутри сети, и ее трудно будет обнаружить средствами превентивной защиты.

2) выполняется первичное проникновение во внутреннюю сеть предприятия с применением методов социальной инженерии и иных нетривиальных методов;

3) производится взлом определенных узлов сети с последующим установлением контроля и распространением влияния злоумышленников в сети атакуемой организации;

4) в итоге всё приводит либо к краже данных, либо к иным несанкционированным действиям с последующим сокрытием следов вредоносной активности в корпоративной сети.

Рис. 1: Стратегия борьбы с целенаправленными атакми.

Классические решения для обеспечения информационной безопасности, внедренные в большинстве крупных компаний по всему миру, нередко хорошо справляются с функцией предотвращения угрозы в пределах периметра корпоративной сети (используя технологии превентивной защиты), но не предназначены для обнаружения угрозы, которая уже может присутствовать в сети продолжительное время, ничем себя не выдавая.

Другими словами, эти решения хорошо выполняют конкретные задачи, но не умеют работать согласованно. По сути, они лишь реализуют функционал противодействия угрозам (NGFW, IDS, Antispam, DLP, SIEM). Однако в современной ситуации всестороннего усложнения ИТ-инфраструктуры — с внедрением виртуализации, использованием мобильных устройств, неконтролируемых способов доступа к интернету — возникают все более изощренные средства доставки вредоносного кода непосредственно внутрь компании, легко обходящие установленные решения превентивной защиты.

Согласно опросу* ИТ-специалистов, лишь 41% компаний обращает должное внимание на развитие существующих подходов для противодействия целевым атакам и лишь 42% дополняют технические средства специальными тренингами для службы ИБ по повышению общей осведомленности о методах социальной инженерии, которые применяются при атаках на рядовых сотрудников. А ведь именно недостаточной продуманностью средств защиты и человеческим фактором стараются воспользоваться злоумышленники при проведении атак.

«Лаборатория Касперского» уже более 10 лет назад, задолго до появления современных целевых атак, разработала и стала использовать внутри компании технологии, позволяющие автоматизировать процесс детектирования вредоносного кода и подозрительной активности, не опираясь на сигнатурный и эвристический анализ. Позднее такая технология появилась на рынке, получив название «песочница» и став полноценным компонентом систем предотвращения целевых атак. «Лаборатория Касперского» ежедневно выявляет 310 000 новых образцов вредоносного кода. Это достигается благодаря экспертизе аналитиков, инновационным технологиям обнаружения, а также интеграции с глобальной репутационной базой угроз Kaspersky Security Network, с помощью которой информация об угрозах поступает со всего мира в режиме реального времени.

Развитие современных угроз и большая потребность в новом подходе подтолкнули «Лабораторию Касперского» к созданию комплексного специализированного решения по противодействию целенаправленным атакам — Kaspersky Anti Targeted Attack Platform.

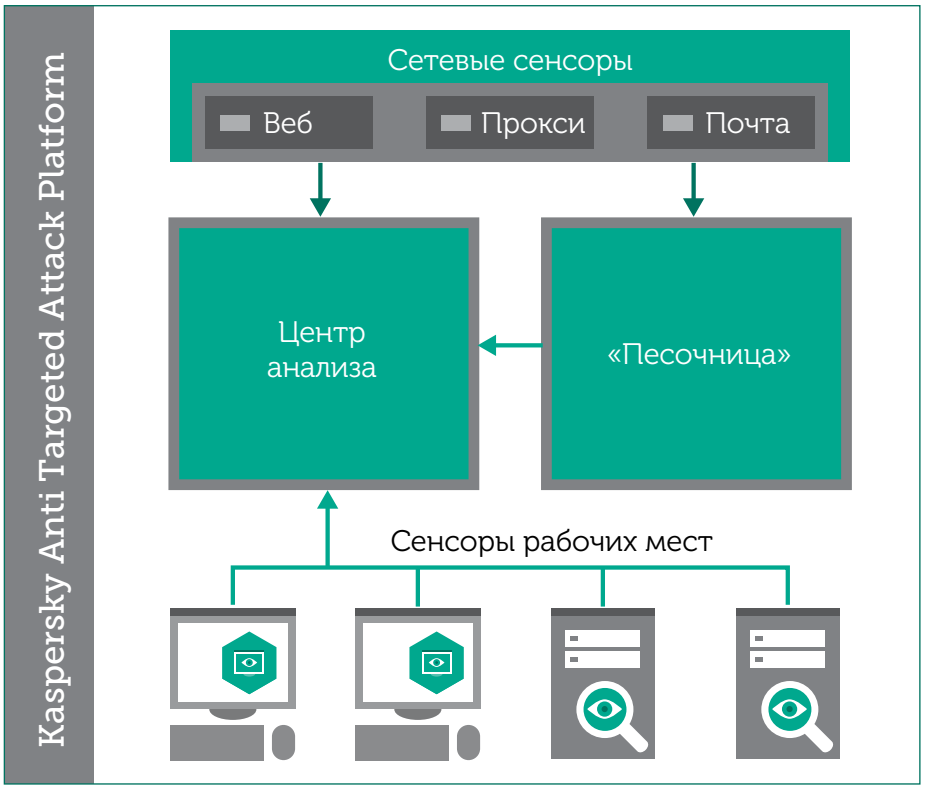
* Ежегодное исследование «Информационная безопасность бизнеса», «Лаборатория Касперского» и B2B International, 2015 год.

СПЕЦИАЛИЗИРОВАННОЕ РЕШЕНИЕ ДЛЯ ПРОТИВОДЕЙСТВИЯ ЦЕЛЕНАПРАВЛЕННЫМ АТАКАМ

Kaspersky Anti Targeted Attack Platform — комплексное решение, ориентированное на средний и крупный бизнес, которое позволяет своевременно обнаруживать целенаправленные атаки и адекватно на них реагировать.

Архитектура решения:

- Сетевые сенсоры, отвечающие за анализ почтового и веб-трафика, в том числе объектов из вложений и веб-контента, получаемых в процессе работы сотрудников в интернете.
- Сенсоры на уровне рабочих станций и серверов («легкие агенты», собирающие информацию о сетевой активности для расследования инцидента).
- Высокопроизводительная «песочница», позволяющая в автоматическом режиме параллельно запускать и изучать потенциально опасные объекты на изолированных виртуальных машинах.



- Центр анализа – механизм оценки и классификации угроз по их уровню критичности, база данных по инцидентам, инструменты визуализации данных и отчетности.
- Эффективное противодействие целенаправленным атакам невозможно осуществить без экспертизы и актуальных сведений о новейших атаках.

Рис. 2: Архитектура решения

Эксперты «Лаборатории Касперского» постоянно изучают технологии подобных угроз и за последние годы выявили десятки крупнейших атак мирового масштаба — Darkhotel, Carbanak и многие другие. А для оперативного получения информации о новых угрозах решение интегрируется с глобальной репутационной базой «Лаборатории Касперского» — Kaspersky Security Network.

- Компании с изолированными сетями могут использовать локальную репутационную базу Kaspersky Private Security Network (KPSN), которая обладает всеми преимуществами облачной сети безопасности, но без передачи данных за пределы корпоративной сети.

- Управление осуществляется через удобный и простой в использовании веб-интерфейс.

ОСНОВНЫЕ ПРЕИМУЩЕСТВА

Модульная архитектура решения не требует внесения изменения (логического либо физического изменения топологии) в существующую ИТ-инфраструктуру компании и органично интегрируется со всеми бизнес-процессами. Детектирующие механизмы Kaspersky Anti Targeted Attack Platform работают с зеркалированным трафиком и не вносят задержек в существующие ИТ-процессы и работу компании. Простой централизованный процесс установки обеспечивает быстрое развертывание и гибкость настройки.

Одной из задач решения является четкий фокус на целевые атаки, конкретизация информации в центре анализа для специалиста по ИТ-безопасности. Решение предоставляет информацию лишь о тех инцидентах, которые связаны с целенаправленными атаками. Для большей информативности все полученные инциденты автоматически классифицируются по уровню опасности. Консоль специалиста по ИТ-безопасности позволяет ему не только получать информацию по выявленной проблеме, но и проводить расследование (почему и на основе каких данных и технологий решение вынесло вердикт, что инцидент связан с целевой атакой). Тем самым снижаются затраты, связанные с необходимостью получения данных от машин, на которых произошел инцидент безопасности.

Решение Kaspersky Anti Targeted Attack Platform не требует удаления существующих защитных решений, дополняя их инструментами обнаружения сетевого уровня и «песочницей». Такой дополнительный уровень позволяет в режиме реального времени на стороне защищаемой инфраструктуры выявлять ранее неизвестные вредоносные программы. В дополнение к этому в составе детектирующих технологий решение имеет встроенную поведенческую модель. Опираясь на получаемые данные, она автоматически создает шаблоны поведения IT-инфраструктуры и указывает на аномалии. В результате подобная технология позволяет не только найти вредоносную и подозрительную активность с позиции информационной безопасности, но и выявлять отклонения, которые часто свидетельствуют о действиях вредоносных программ по сокрытию следов своего присутствия от средств защиты.

Для заказчиков, владеющих SIEM- или SOC-системами, в рамках которых организованы процессы обнаружения сложных современных угроз, Kaspersky Anti Targeted Attack Platform позволяет передавать аналитику по инцидентам для повышения качества обнаружения угроз. Также с этой целью можно использовать сервисы информирования об угрозах и аналитические отчеты «Лаборатории Касперского».

ЭКСПЕРТИЗА В ОБЛАСТИ КИБЕРБЕЗОПАСНОСТИ

Статистика целевых атак показывает, что даже наличие эффективной технологии детектирования (например, «песочницы» на уровне периметра сети) не является панацеей от всех угроз. Необходимо правильно классифицировать выявленные инциденты и реагировать на них в соответствии с уровнем опасности, что в текущих реалиях требует высокой квалификации сотрудников служб ИБ, специальных знаний при проведении расследований и опыта выявления целевых атак.

«Лаборатория Касперского» дополняет свое решение всеми необходимыми экспертными сервисами для построения полноценного процесса противодействия целевым атакам на стороне организации.

- **Повышение осведомленности о киберугрозах.** Правильно ли действуют сотрудники с точки зрения информационной безопасности? Могут ли они определить, что получили сообщение от злоумышленников или вредоносную ссылку? Готовы ли противостоять методам социальной инженерии? Специализированные курсы «Лаборатории Касперского» позволяют существенно уменьшить негативное влияние человеческого фактора (вариант целевого тренинга и удаленного обучения в виде игры).

Выявление сложных современных угроз и реагирование на них требует глобальной осведомленности и экспертных знаний

- **Программа экспертного обучения в области ИБ.** Обучение специалистов ИБ основам и практическим навыкам организации стратегии информационной безопасности с учетом сложных современных угроз и рисков целевых атак.

- **Специализированные тренинги.** Проводятся для специалистов служб ИБ (операторов решения по противодействию целевым атакам) и обучают как реагированию на инциденты, так и методам проведения полноценного расследования.

- **Сервис реагирования на инциденты.** В случае если у заказчика возникает ИБ-инцидент (выявленный Kaspersky Anti Targeted Attack Platform или иным путем), эксперты «Лаборатории Касперского» помогут не только провести расследование, но и разработать правильные шаги по решению проблемы.

- **Сервис обнаружения целенаправленных атак.** Для заказчиков, которые пока не готовы использовать специализированное решение, эксперты «Лаборатории Касперского» могут провести разовый анализ инфраструктуры с целью выявления уже действующей в сети целевой атаки или ее следов.

Решения для крупного бизнеса: kaspersky.ru/enterprise-security

KASPERSKY lab