KASPERSKY lab

KASPERSKY ANTI TARGETED ATTACK PLATFORM

Надежная система обнаружения целевых атак «Лаборатории Касперского»

www.kaspersky.com

ВВЕДЕНИЕ

«Лаборатория Касперского» год от года обнаруживает все больше целевых атак. В ближайшее время этот тренд не изменится, и количество атак будет только расти. Службам информационной безопасности предприятий необходимо учитывать это при создании или обновлении своих систем безопасности. Игнорирование проблемы чревато огромными финансовыми и репутационными потерями, как видно на примерах не только коммерческих компаний, но даже госорганов и подрядчиков стратегических проектов.

Учитывая количество атак, отдельной задачей становится автоматизация их обнаружения. Еще в 2008 году «Лаборатория Касперского» создала специализированное подразделение для противодействия сложным целевым угрозам — глобальный центр исследований и анализа угроз (GReAT). Именно поэтому сегодня наши аналитики обладают самым обширным опытом выявления целенаправленных атак.

Мы воплотили этот опыт и инструменты обнаружения атак в виде отдельного решения — ***Kaspersky Anti Targeted Attack Platform***. Оно сочетает обширную базу знаний в области изучения и выявления угроз, накопленную за последний десяток лет, с проверенными эффективными технологиями. Платформа непрерывно анализирует сетевой и почтовый трафик, выделяя, классифицируя и проверяя содержащиеся в нем объекты. Метаданные и объекты при этом сохраняются, а затем анализируются и сопоставляются для выявления признаков атаки.

Необходимым условием правильной работы решения является его профессиональная настройка, обучение сотрудников взаимодействию с системой и реагированию на киберинциденты. Такие услуги составляют неотъемлемую часть решения Kaspersky Anti Targeted Attack Platform, и «Лаборатория Касперского» предоставляет их одновременно с поставкой продукта.

МОДУЛИ СБОРА ДАННЫХ

За сбор данных отвечают несколько типов сенсоров, анализирующих разнородный трафик (http, smtp и др.). При развертывании Kaspersky Anti Targeted Attack Platform конфигурация решения может гибко варьироваться в зависимости от каждой конкретной инсталляции. Такой подход, с одной стороны, позволяет защитить корпоративную IT-инфраструктуру любой сложности и конфигурации (в том числе использующую сторонние защитные решения — например, на конечных устройствах), разместив нужные сенсоры в ее ключевых точках, а с другой — сократить бюджет внедрения. Экономия достигается за счет того, что при наличии сенсоров пропадает необходимость целиком разворачивать отдельное решение для каждого канала передачи данных. Все сенсоры работают одновременно и независимо друг от друга.

Сетевые сенсоры

За годы борьбы с вредоносным ПО «Лаборатория Касперского» накопила огромный объем данных о «зловредах» и легитимных файлах, подозрительном поведении программ, доверенных и вредоносных сетевых адресах. Kaspersky Anti Targeted Attack Platform использует все эти данные для выявления вторжений, анализа сетевого трафика и обработки выделенных объектов в песочницах.

Сетевые сенсоры, основанные на индустриальном стандарте подобных решений, отвечают за сбор данных из сетевого трафика.

Они перехватывают «сырые» данные посредством виртуального сетевого драйвера TAP или Switched Port Analyzer (SPAN). На уровне приложений анализируются такие протоколы, как HTTP, FTP и DNS. Просматривая весь поток данных, сенсоры генерируют описывающие его **метаданные**, а также выделяют из трафика **объекты**. После этого метаданные и выделенные объекты анализируются с помощью разных модулей центра анализа.

Веб-сенсоры

Помимо сетевых сенсоров, в Kaspersky Anti Targeted Attack Platform отдельно выделяются **веб-сенсоры**. Они отличаются способом сбора данных и применяются в том случае, когда инфраструктура компании не позволяет забирать трафик через SPAN-порт. Например, это происходит, когда зашифрованный сетевой https-трафик в открытом виде существует только на корпоративном прокси-сервере компании[1]. Именно с него по протоколу ICAP он может попасть на анализ в Kaspersky Anti Targeted Attack Platform. Такая конфигурация позволяет обнаруживать атаки, в которых для связи зараженных хостов с управляющими серверами или загрузки дополнительных модулей используется https.

Но это не единственный сценарий использования сетевых сенсоров. Они могут применяться в любой архитектуре, когда использовать ICAP по каким-то причинам удобнее, чем SPAN.

Почтовые сенсоры

Подавляющее большинство целевых атак начинается с детально проработанной рассылки писем (spear-phishing). Не надо думать, что попасться на такой трюк злоумышленников могут только неподготовленные сотрудники. Предварительная разведка позволяет атакующим отправлять письма, которые с большой долей вероятности приводят к открытию файла или переходу по ссылке даже подготовленными менеджерами высшего звена и специалистами по ИБ. Достаточно взглянуть на цели атаки Pawn Storm, включавшие американский Белый дом, и на то, как составлялись эти письма — в полном соответствии с текущей политической повесткой дня.

Таким образом, модуль наблюдения за электронной почтой является обязательной частью комплексного решения. Почтовый сенсор позволяет контролировать пересылку писем с вложениями. Для настройки таких сенсоров копия той части корпоративной переписки, которая должна проверяться, отправляется через BCC в выделенный ящик, контролируемый сенсорами. Этот механизм позволяет отбирать для проверки строго определенные почтовые ящики. Специалист по ИБ сможет настроить сенсор таким образом, чтобы он игнорировал служебные учетные записи, на которые поступают автоматизированные отчеты и предупреждения. За редким исключением такие ящики не получают фишинговых писем.

1 В этом случае в конкретной сети применяется контроль зашифрованного трафика или так называемый Corporate Man-in-the-Middle.

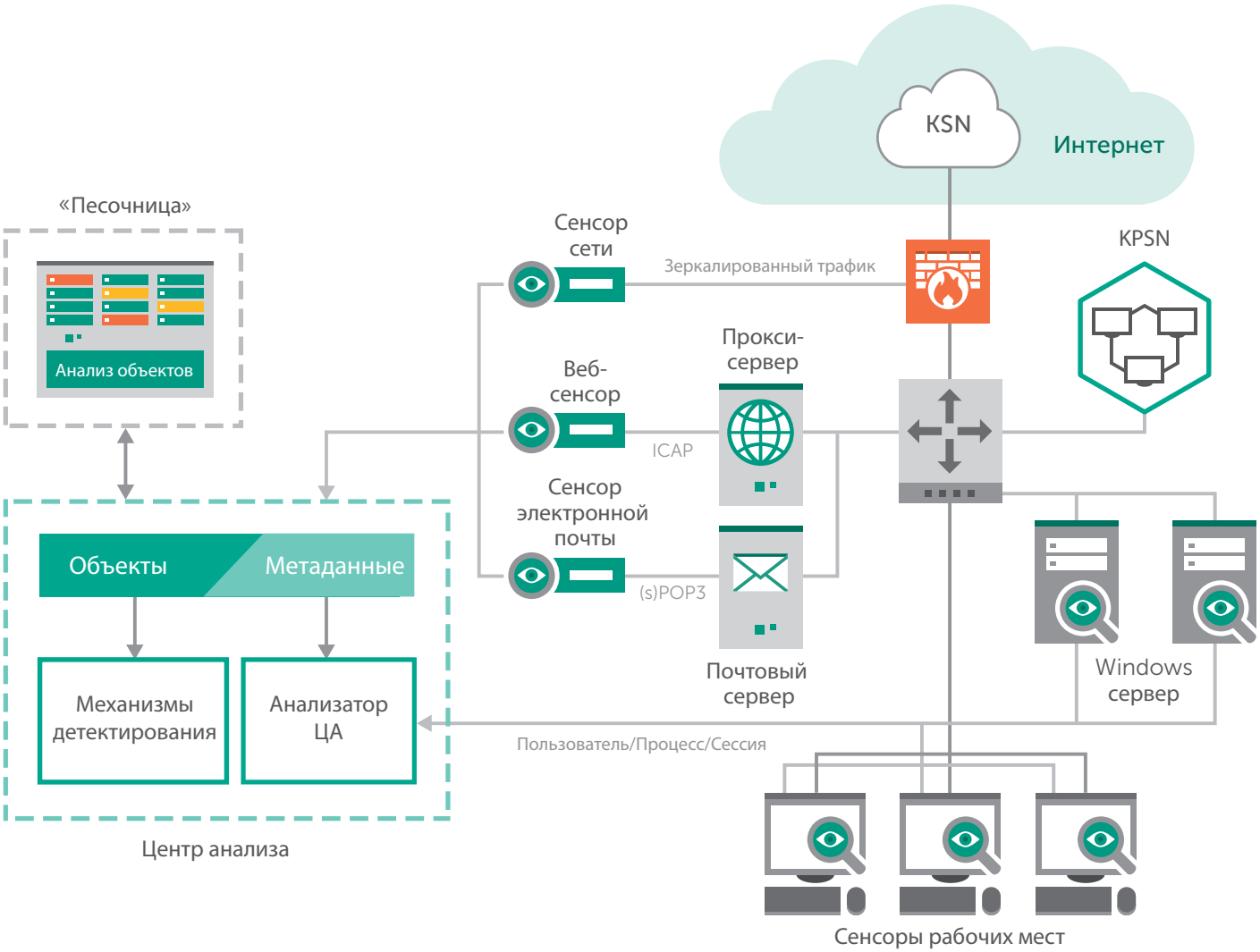
Сенсоры рабочих станций

В отличие от типов сенсоров, перечисленных выше, отказ от которых хотя и возможен, но сразу же повлияет на общую защищенность инфраструктуры, **сенсоры рабочих станций** — действительно опциональны. Отсутствие, например, почтовых сенсоров автоматически означает отсутствие контроля за почтовым трафиком. Без сенсоров рабочих станций общая безопасность не страдает, тем не менее они дают Kaspersky Anti Targeted Attack Platform ценную дополнительную информацию о происходящем на конечных устройствах. Такие сенсоры осуществляют сбор информации о сетевом поведении процессов на конкретных рабочих станциях.

Именно сенсоры рабочих станций позволяют узнать, какие процессы генерируют подозрительный трафик. Сведение воедино этих данных об активности процессов на хостах и информации, полученной из сетевого трафика, позволяет Kaspersky Anti Targeted Attack Platform подробно сообщать обо всем, происходящем в инфраструктуре, сотрудникам службы информационной безопасности.

Сенсоры рабочих станций представляют собой «легкие агенты», работа которых почти не сказывается на производительности конечного устройства. Кроме того, они могут работать параллельно с большинством распространенных ИБ-решений других вендоров без каких-либо проблем совместимости.

Основная цель сбора информации сенсорами всех типов — ее последующий автоматический анализ и предоставление пользователю в удобном виде. И здесь мы подходим ко второму блоку модулей Kaspersky Anti Targeted Attack Platform – **центру анализа**. В нем ведется дальнейшая обработка согласно типу обнаруженных объектов. В состав Kaspersky Anti Targeted Attack Platform входит множество технологий «Лаборатории Касперского» и в зависимости от типа объектов задействуются соответствующие подсистемы. Например, исполняемые файлы открываются в «песочнице», но JavaScript и другие интерпретируемые языки программирования обрабатываются специализированными системами.


KSN
Интернет
«Песочница»
Анализ объектов
Сенсор сети
Зеркалированный трафик
KPSN
Прокси-сервер
Веб-сенсор
ICAP
Сенсор электронной почты
(s)POP3
Объекты
Метаданные
Механизмы детектирования
Анализатор ЦА
Центр анализа
Почтовый сервер
Windows сервер
Пользователь/Процесс/Сессия
Сенсоры рабочих мест

ЦЕНТР АНАЛИЗА

«Песочница»

Для анализа вредоносности файла его нужно запустить на исполнение. Динамический анализ выделенных сенсорами объектов происходит на изолированных виртуальных машинах с различными ОС и наборами прикладного ПО — так называемых песочницах. Таким образом центр анализа контролирует реальное поведение подозрительной программы, но при этом не позволяет «зловреду» вырваться за пределы виртуальной среды и заразить инфраструктуру компании.

Обратной стороной такого метода динамического анализа является то, что продвинутое вредоносное ПО контролирует свой запуск на виртуальных машинах и может никак не проявлять себя. В таком случае недостаточно просто развернуть необходимое заказчику число виртуальных машин с нужными ОС. Наша «песочница» создана таким образом, чтобы в некоторых случаях помешать вредоносному ПО распознать виртуальную среду – так оно не может скрыть свое присутствие.

Некоторые техники обнаружения виртуальных машин, применяемые вредоносным ПО, напротив, приводят к обратному эффекту — «песочница» обнаруживает попытку обнаружить исполнение в виртуальной среде и экстренно завершиться. Именно благодаря этому делается вывод о вредоносности проверяемого приложения.

Как и в случае с сенсорами, количество виртуальных машин гибко варьируется и определяется для каждого проекта отдельно.

Ядра обработки объектов и метаданных

Этот модуль объединяет целый ряд технологий, которые обеспечивают надежное обнаружение угроз различного уровня на основе данных, полученных от сенсоров.

Основанная на отраслевых стандартах система обнаружения вторжения (IDS) включает уникальный набор правил, разработанных «Лабораторией Касперского». Это позволяет ей распознавать вредоносное сетевое поведение и самостоятельно выявлять «зловредов». Кроме того, признаки угроз могут быть добавлены в систему в виде YARA-правил, описывающих известные активные целевые атаки. Также специально для Kaspersky Anti Targeted Attack Platform нами была разработана технология анализа Android-приложений **Risk Score**, оценивающая уровень подозрительности .apk-файлов.

Для оценки благонадежности URL-адресов и файлов используется вся база знаний, накопленная Kaspersky Security Network. В число систем обработки также входит антивирусное ядро «Лаборатории Касперского» с эвристическими механизмами нового поколения и технологией машинного обучения. Это способствует эффективному обнаружению как уже известных, так и новых угроз. Объектами анализа антивирусного ядра могут быть не только динамически присоединяемые библиотеки, но также скрипты на различных интерпретируемых языках и другие объекты разных форматов, потенциально способные нанести вред.

Несмотря на то, что Kaspersky Security Network полностью обезличивает всю обрабатываемую информацию, некоторые компании в силу требований нормативных актов или корпоративной политики нуждаются в абсолютном отказе от исходящего трафика во внешние облачные системы.

Таким компаниям «Лаборатория Касперского» предлагает отдельный продукт — **Kaspersky Private Security Network**. При использовании этого решения ни один бит данных о найденных угрозах не уходит из сети предприятия наружу, даже в дата-центры «Лаборатории Касперского», что никак не отражается на доступности глобальной облачной базы знаний. Иными словами, компания получает в свое распоряжение локальную версию Kaspersky Security Network[2].

Анализатор целевых атак

В модуле Targeted Attack Analyzer (анализатор целенаправленных атак) проводится уникальный статистический анализ сетевого трафика для поиска аномалий. Этот модуль знает, какая активность типична для данной инфраструктуры, и подозрительное отклонение от обычной картины является поводом для тревоги. Для работы анализатор целевых атак пользуется базой знаний о глобальной популярности доменов и whois-данными.

Однако, помимо общемировых данных, модуль «помнит» популярность доменов и для конкретной компании-заказчика. К примеру, внезапный переход на домен, недавно созданный в стране, трафик в которую из периметра безопасности раньше замечен не был, станет основанием для предупреждения.

2 Доступ к базе знаний является залогом эффективной работы Kaspersky Targeted Attack Platform. Если ваша компания по соображениям безопасности не может работать с внешними базами, то мы рекомендуем развернуть локальную репутационную базу Kaspersky Private Security Network.

Анализатор целенаправленных атак использует передовые технологии интеллектуального анализа и машинного обучения, обеспечивая быстрое обнаружение подозрительного поведения в сети заказчика. Использование машинного обучения помогает «Лаборатории Касперского» формировать собственные базы данных для эвристического анализа, использующиеся при кластеризации образцов на основе коэффициента сходства с уже кластеризованными файлами.

База знаний об угрозах

Одним из главных преимуществ Kaspersky Anti Targeted Attack Platform является возможность использования всего арсенала технологий «Лаборатории Касперского». Благодаря Kaspersky Security Network платформа получает доступ к нескольким глобальным базам данных, в которых содержится информация:

- о репутации URL-адресов и файлов, позволяющей делать выводы о подозрительности трафика и объектов;
- об активных командных серверах активных атак;
- об источниках распространения вредоносного ПО и т. д.

База данных постоянно пополняется в режиме реального времени. Уникальным источником данных для Kaspersky Anti Targeted Attack Platform является перечень доменов, используемых активными целевыми атаками. Данные о них поддерживает в актуальном состоянии команда глобального центра исследований и анализа угроз (GReAT) «Лаборатории Касперского». Kaspersky Anti Targeted Attack Platform эффективно выявляет угрозу, как только встречает в трафике упоминание хоста, связанного с известной целевой атакой.

Не стоит забывать и о том, что даже самый совершенный продукт должен быть правильно установлен (выбраны корректные сегменты корпоративной сети, расположение оборудования для развертывания решения и т. п.) и регулярно обслуживаться подготовленными сотрудниками компании. «Лаборатория Касперского» вместе с решением предлагает услуги по развертыванию, тренинги по работе с продуктом и реагированию на инциденты. Кроме того, все собранные и автоматически проанализированные данные должны быть представлены в удобном виде. Для этого в Kaspersky Anti Targeted Attack Platform есть встроенные возможности **визуализации и интеграции** со сторонними решениями.

Консоль

Комплексность современной эффективной системы для борьбы с целевыми атаками обуславливает необходимость получения всех данных в **едином центре**. Вся собранная и проанализированная информация должна предоставляться сотруднику службы безопасности централизованно и в удобном виде. Именно за это отвечает консоль управления. Важной функцией базы данных вердиктов, наполняемой всеми ядрами, является **ретроспективный поиск**. Гибкая фильтрация событий, зарегистрированных разными модулями, может помочь восстановить их хронологию и проследить зависимости.

В базе данных вердиктов сохраняются все сведения о событиях в корпоративной IT-инфраструктуре. На самом высоком уровне детализации используются **журналы** с записями о каждом событии. Такие записи позволяют проводить расследование с целью установления детальной истории атаки. Существуют разные форматы журналов, так как с одной стороны нужно сохранять детальные данные для расследований, а с другой — их сокращенный вариант для быстрого поиска и долгосрочного хранения. Для этого используются **метки времени** (создание записей за определенный период), записи **по факту** (относящиеся к конкретному локальному хосту, удаленному хосту и процессу — все три должны быть задействованы в событии). Кроме того, некоторые обнаруженные объекты — например объекты, выделенные в ходе работы песочницы, — также сохраняются в течение некоторого времени.

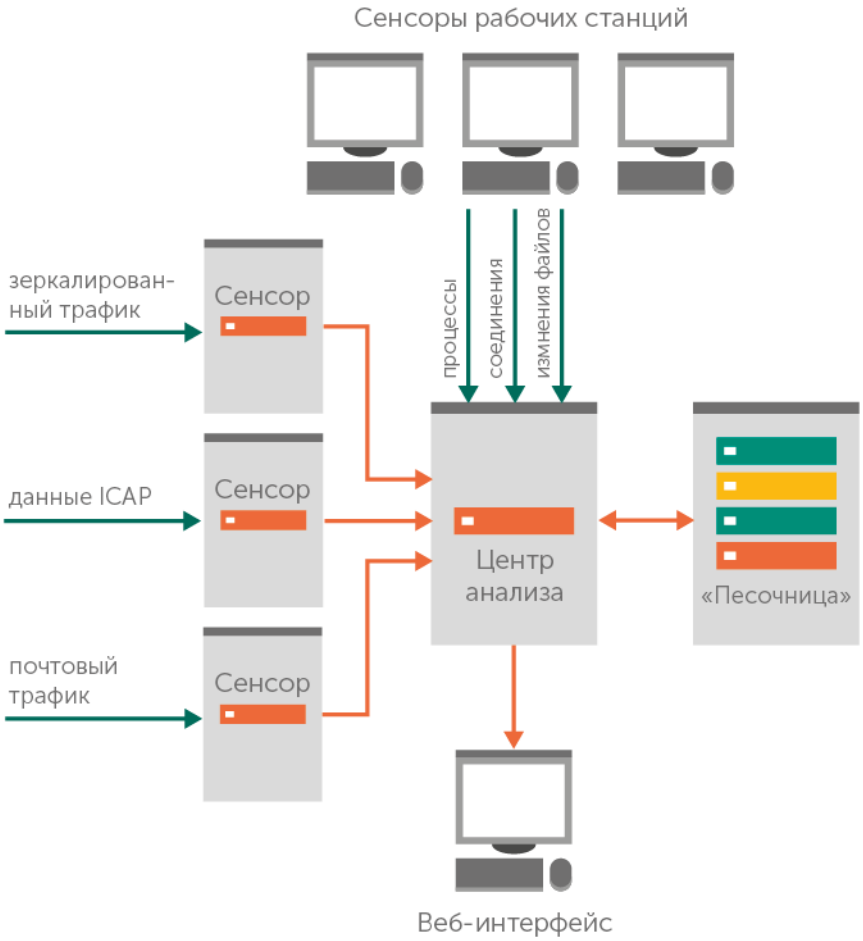
Сторонние SIEM

Помимо работы в собственной консоли, данные из Kaspersky Anti Targeted Attack Platform можно выгружать в сторонние SIEM. Kaspersky Anti Targeted Attack Platform выдает их в популярном формате syslog, данные в котором затем могут быть импортированы в HP ArcSight, IBM Qradar, Splunk и любое другое популярное SIEM-решение.

Схема использования оборудования

Для развертывания Kaspersky Anti Targeted Attack Platform требуется не менее двух серверов. В этом случае все сенсоры, кроме сенсоров рабочих станций, будут работать на одном сервере.

Для полноценного развертывания в корпоративной среде потребуется четыре сервера и более. В этом случае сенсоры будут распределены между серверами.



Заключение

Сложность современных атак влечет за собой необходимость использования комплексных защитных решений. Службы информационной безопасности предприятий не могут ограничиться защитой только части систем или анализом только некоторых признаков. Внимания требует все. В противном случае практически неизбежны финансовые или репутационные потери.

Мы в «Лаборатории Касперского» придерживаемся следующей модели многоуровневой защиты. Различные виды сканеров собирают «сырые» данные о происходящем в периметре безопасности. Из почтового и веб-трафика выделяются объекты, которые теоретически могут оказаться вредоносными. За их всестороннюю проверку отвечает центр анализа, пользующийся для этого в том числе данными из глобального облака «Лаборатории Касперского».

Решение Kaspersky Anti Targeted Attack Platform до недавней поры существовало как внутренняя экспертная система обнаружения атак, которой до этого пользовались только сотрудники «Лаборатории Касперского». Теперь организации получают доступ к нашим наработкам, основанным на многолетнем опыте борьбы не только с вредоносными программами, но и с целевыми атаками.

Решения для защиты крупного бизнеса: kaspersky.ru/enterprise