kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Threat Attribution Engine

Киберугрозы постоянно эволюционируют. Наблюдать за ними, анализировать, вовремя реагировать на атаки и сводить к минимуму их последствия – чрезвычайно трудоемкий процесс. Аналитика угроз – не просто модное направление в информационной безопасности, это важный инструмент защиты. Одна из самых громких и спорных тем в этой области – атрибуция угроз.

Основные характеристики продукта:

- Мгновенный доступ к хранилищу, где содержатся коллекции данных о сотнях APT-компаний и множестве экземпляров вредоносного ПО
- Эффективная приоритизация угроз и классификация событий в автоматическом или ручном режиме
- Возможность добавлять киберпреступников и образцы, чтобы система научилась распознавать аналогичные экземпляры
- Добавление экземпляров вручную и открытый интерфейс API для интеграции с автоматизированными процессами
- Возможность развертывания в изолированной среде для защиты систем и данных, а также для соблюдения нормативных требований
- Абсолютная конфиденциальность всех загружаемых документов, предотвращающая утечку секретной информации

Атрибуция угроз заслужила такое внимание по вполне понятной причине. Сложные методы расследования и обратной разработки замедляют реагирование на продвинутые угрозы, и часто злоумышленники успевают достичь своей цели. Корректная и своевременная атрибуция сокращает время реагирования на инцидент с нескольких часов до нескольких минут, а также снижает количество ложноположительных срабатываний.

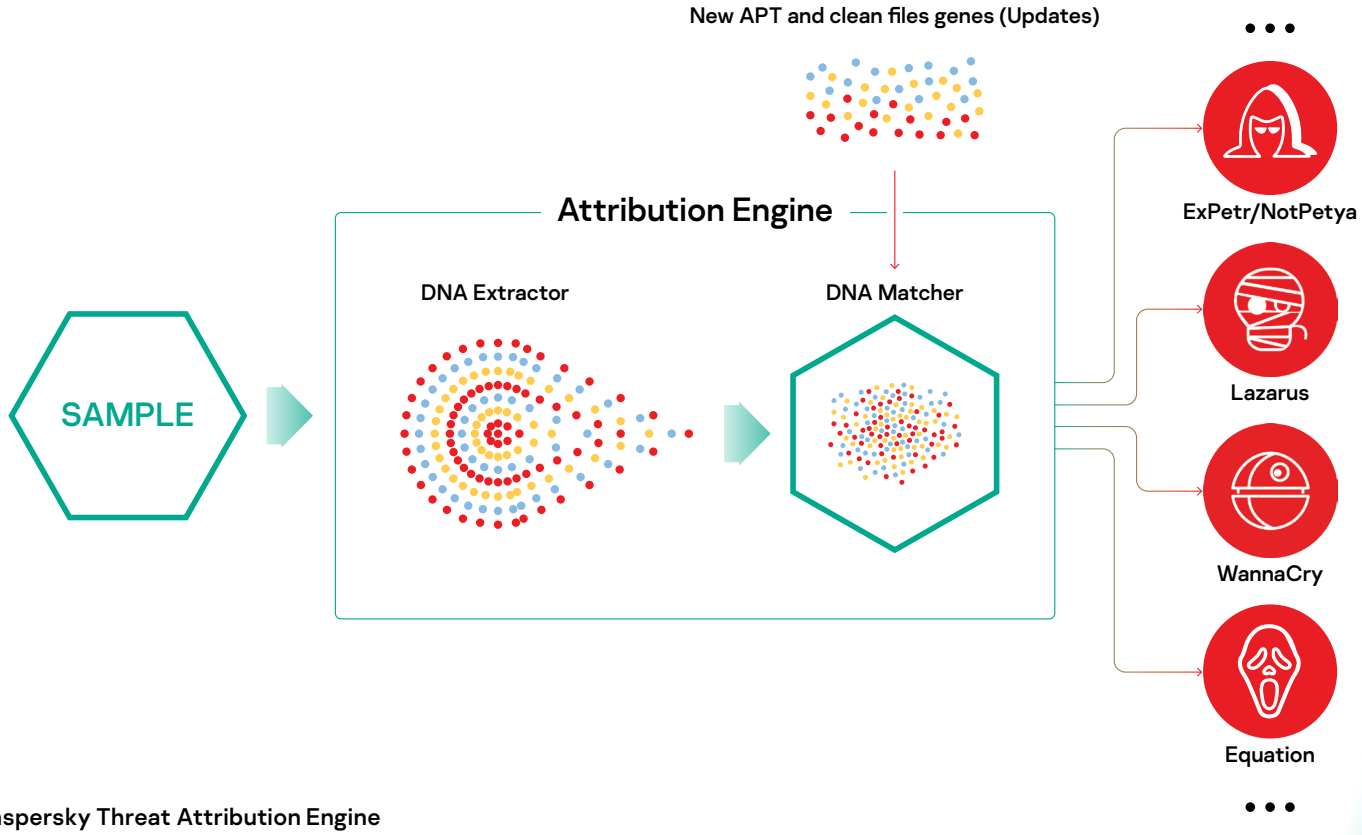
Обнаружение целевой атаки, профилирование моделей поведения и разработка факторов атрибуции для различных угроз – трудоемкая и тщательная работа, на которую можно потратить годы. Чтобы создать эффективную систему атрибуции, необходимы высококвалифицированные специалисты с опытом расследования инцидентов безопасности и большие объемы данных, накопленные за много лет. Эта группа исследователей будет наблюдать за деятельностью киберпреступных группировок и постепенно пополнять базу данных. Со временем накопленная информация станет ценным ресурсом и принесет пользу множеству организаций.

База данных Kaspersky Threat Attribution Engine содержит экземпляры APT-угроз и чистые файлы, собранные экспертами «Лаборатории Касперского» за 22 года. Мы отслеживаем более 600 киберпреступников и APT-кампаний и ежегодно составляем более 120 аналитических отчетов. Непрерывные исследования помогают пополнять огромную библиотеку APT-угроз актуальным данными: сегодня она содержит более 60 тысяч файлов. Благодаря этому система атрибуции эффективнее отслеживает отвлекающие маневры и с помощью автоматизированных инструментов максимально точно определяет источник угроз.

В продукте используется уникальный метод сравнения экземпляров и выявления сходств между ними. Вероятность ложноположительного срабатывания при этом минимальна. Система атрибуции «Лаборатории Касперского» сопоставляет новые события с известными APT-угрозами, целевыми атаками и киберпреступными группировками, позволяя отличить серьезные случаи от незначительных инцидентов и вовремя остановить злоумышленника, не дав ему получить доступ к системе.

Принцип работы

Kaspersky Threat Attribution Engine проводит «генетический анализ» вредоносных программ: система автоматически находит сходства с экземплярами уже расследованных APT-атак и сопоставляет с данными о киберпреступниках. Система атрибуции сравнивает «генотипы» (бинарные фрагменты файлов) с базой экземпляров APT-угроз, затем составляет отчет о происхождении вредоносного ПО и схожести файлов с экземплярами известных APT-угроз. Кроме того, специалисты могут добавлять киберпреступников и объекты в базу данных системы, таким образом обучая ее распознавать аналогичные экземпляры. Благодаря Kaspersky Threat Attribution Engine процесс занимает считаные секунды, а не годы, как это было раньше.



Kaspersky Threat Attribution Engine

Систему можно развернуть в изолированной среде, защищенной от доступа сторонних лиц к обрабатываемой информации и отправляемых в нее объектах. Интерфейс API позволяет подключиться к другим инструментам и фреймворкам, чтобы внедрить атрибуцию в существующую инфраструктуру и автоматизированные процессы.

Подробную информацию о соответствующей APT-группировке можно найти в аналитических отчетах «Лаборатории Касперского» об APT-угрозах[1]. Подписчики получают в различных форматах уникальный доступ к результатам расследования и техническим данным по каждой APT-угрозе сразу после их появления, даже если они никогда не будут опубликованы.

Kaspersky Threat Attribution Engine значительно упрощает управление безопасностью за счет следующих свойств:

- Быстрая атрибуция файлов известных APT-группировок, позволяющая распознать цели, методы и инструменты кибератаки
- Быстрый анализ, позволяющий применить необходимые процедуры сдерживания и реагирования в зависимости от степени риска (целенаправленная атака или случайная жертва)
- Эффективное и своевременное предотвращение атаки на основе актуальных аналитических данных об APT-угрозах, представленных в отчетах «Лаборатории Касперского»

1 Подписка на аналитические отчеты об APT-угрозах приобретается отдельно

www.kaspersky.ru