Kaspersky Threat Attribution Engine

kaspersky BRING ON THE FUTURE

Эволюция киберугроз

Киберугрозы постоянно эволюционируют. Наблюдать за ними, анализировать, вовремя реагировать на атаки и сводить к минимуму их последствия – чрезвычайно трудоемкий процесс.

Kaspersky Threat Attribution Engine

Целевые атаки – одна из главных угроз для организаций. Обычно такие атаки тщательно готовятся, и злоумышленники используют самые разные техники и тактики, чтобы причинить вред и при этом как можно дольше остаться незамеченными. Атрибуция угроз позволяет понять, кто стоит за целевой атакой, что является ее первоочередной целью и какие инструменты и методы обычно использует та или иная кибергруппировка, чтобы достичь нужного ей результата. Все это помогает быстрее и точнее реагировать на инцидент, уменьшать негативные последствия атаки и проводить эффективные расследования.

При этом, чтобы создать эффективную систему атрибуции, необходимы высококвалифицированные специалисты с опытом расследования инцидентов безопасности и большие объемы данных, накопленные за много лет. Эксперты «Лаборатории Касперского» за годы работы обнаружили десятки атак глобального масштаба, проводят скрупулезные исследования APT-атак и постоянно изучают новые угрозы. Эти обширные знания легли в основу Kaspersky Threat Attribution Engine.

База знаний Kaspersky Threat Attribution Engine содержит информацию об экземплярах вредоносных объектов, ассоциированных с известными «Лаборатории Касперского» APT-угрозами, собранными за более чем 20 лет работы, и оперативно пополняется. Доступ к уникальным данным об угрозах позволяет аналитикам безопасности обеспечить своевременную реакцию на сложные APT-кампании и скорректировать существующие подходы к организации защищаемой инфраструктуры.

600+

киберпреступников и APT-кампаний мы отслеживаем

120+

аналитических отчетов составляем ежегодно

60 000+

файлов содержит сегодня библиотека APT-угроз

База данных

База знаний Kaspersky Threat Attribution Engine содержит информацию об экземплярах вредоносных объектов, собранных за более чем 20 лет работы

В решении используется уникальный метод сравнения анализируемых экземпляров подозрительных файлов с вредоносными образцами из коллекции Лаборатории Касперского», в целях выявления степени схожести 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.

Основные характеристики продукта

Доступ к базе знаний

Мгновенный доступ к хранилищу, где содержатся коллекции данных о сотнях APT-компаний и множестве экземпляров вредоносного ПО

Экспорт правил YARA

Экспорт правил YARA для дальнейшего автоматизированного поиска похожих файлов в инфраструктуре

Интеграция со сторонними системами

Добавление экземпляров вручную и открытый интерфейс API для интеграции с автоматизированными процессами

Работа в изолированной среде

Возможность развертывания в изолированной среде для защиты систем и данных, а также для соблюдения нормативных требований

Поддержка разных форматов

Экспорт в формат STIX 2.1 (также поддерживаются форматы TXT и JSON) для дальнейшего автоматизированного анализа журналов безопасности и для интеграции со сторонними решениями и средствами безопасности

Пополнение базы знаний

Возможность добавлять исполнителей угроз и образцы, чтобы система научилась распознавать аналогичные экземпляры

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.

Благодаря Kaspersky Threat Attribution Engine процесс занимает считаные секунды, а не годы, как это было раньше.

Специалисты могут добавлять киберпреступников и объекты в базу данных системы, таким образом обучая ее распознавать аналогичные экземпляры.

Систему можно развернуть в изолированной среде, защищенной от доступа сторонних лиц к обрабатываемой информации и отправляемым в нее объектам. Интерфейс API позволяет подключиться к другим инструментам и фреймворкам, чтобы атрибуция угроз стала частью существующих процессов IT-безопасности.

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, в том числе закрытым и не планируемым к публикации «Лабораторией Касперского».

[1]Подписка на аналитические отчеты об APT-угрозах приобретается отдельно

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»

Kaspersky Threat Intelligence

FORRESTER®

«Лаборатория Касперского» признана лидером по результатам исследования внешних сервисов анализа угроз (Forrester Wave™: External Threat Intelligence Services, Q1 2021)

«Лаборатория Касперского» предлагает сервисы информирования об угрозах, которые открывают доступ к различной информации, полученной нашими аналитиками и исследователями мирового класса. Эти данные помогут любой организации эффективно противостоять современным киберугрозам.

Наша компания обладает глубокими знаниями, богатым опытом исследования киберугроз и уникальными сведениями обо всех аспектах IT-безопасности. Благодаря этому «Лаборатория Касперского» стала доверенным партнером правоохранительных и государственных организаций по всему миру, в том числе Интерпола и различных подразделений CERT. Kaspersky Threat Intelligence предоставляет актуальные технические, тактические, операционные и стратегические данные об угрозах.

Kaspersky Threat Intelligence

Подробнее

www.kaspersky.ru