Sandbox

Attribution

Similarity

Kaspersky Threat Analysis

kaspersky активируй будущее

Kaspersky Threat Analysis

Kaspersky Threat Analysis

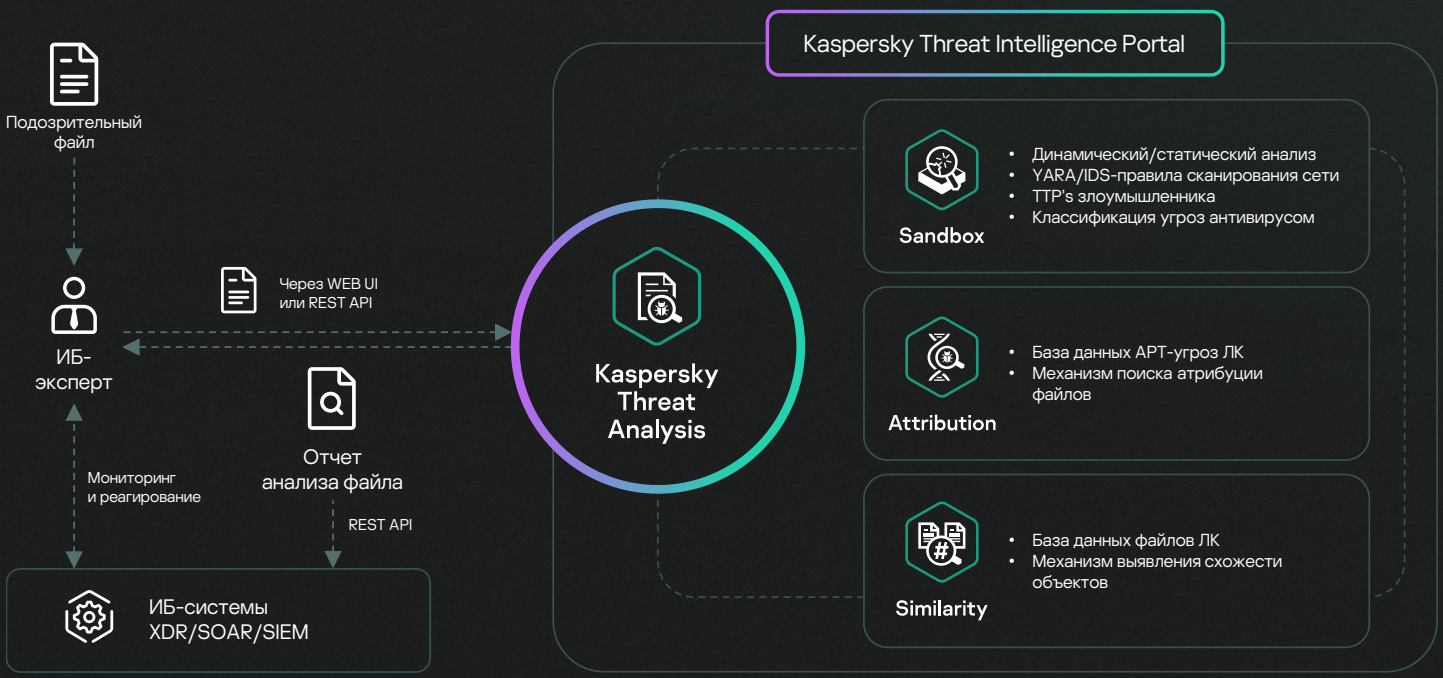
В борьбе с киберугрозами критически важно быстро и эффективно принять решение по противодействию им. Уже невозможно предотвратить современные целевые атаки только с помощью традиционного антивируса. Стандартные механизмы антивирусной защиты способны блокировать в основном известные угрозы (с минимальным поведенческим анализом), в то время как целенаправленно действующие злоумышленники используют все имеющиеся в их арсенале средства с целью избежать автоматического обнаружения. Количество ИБ-событий, ежедневно обрабатываемых SOC, растет в геометрической прогрессии. Учитывая количество ежедневно появляющихся образцов ВПО, эффективная приоритезация и своевременная работа по инцидентам без современных автоматизированных средств анализа становится практически невыполнимой задачей.

Kaspersky Threat Analysis предоставляется в виде облачного сервиса с доступом через Kaspersky Threat Intelligence Portal. Благодаря единой точке доступа, технологии работают взаимосвязанно, обогащая и усиливая друг друга.

Мощный инструмент для комплексного анализа угроз Kaspersky Threat Analysis предоставит данные для принятия обоснованных решений, эффективного сдерживания угроз и выведет процесс расследования инцидентов на новый уровень. Помимо облачной песочницы, сервис предоставляет доступ к самым современным технологиям атрибуции кибератак и выявления схожести подозрительных файлов с другими известными вредоносными объектами.

С помощью технологий, входящих в Kaspersky Threat Analysis, ваши аналитики смогут всесторонне оценить ситуацию, получить полное представление о ландшафте угроз и принять эффективные и своевременные меры реагирования.

Схема работы Kaspersky Threat Analysis



Мощный инструмент динамического анализа, позволяющий исследовать исходные образцы файлов, находить индикаторы компрометации на основании поведенческого анализа и обнаруживать вредоносные объекты, которые не встречались ранее.

Sandbox

Песочница «Лаборатории Касперского» объединяет все знания о поведении вредоносного ПО, полученные более чем за 25 лет непрерывного исследования угроз, что позволяет обнаруживать более 420 000 новых вредоносных объектов каждый день. Sandbox сочетает в себе поведенческий анализ, надежные техники предотвращения уклонения от анализа и технологии моделирования поведения человека.

Какую проблему решает?

Подозрительные файлы, не обнаруженные антивирусными средствами, могут проявить свое вредоносное поведение только в процессе выполнения. Sandbox позволяет воспроизвести поведение файла и выявить любую потенциально опасную активность.

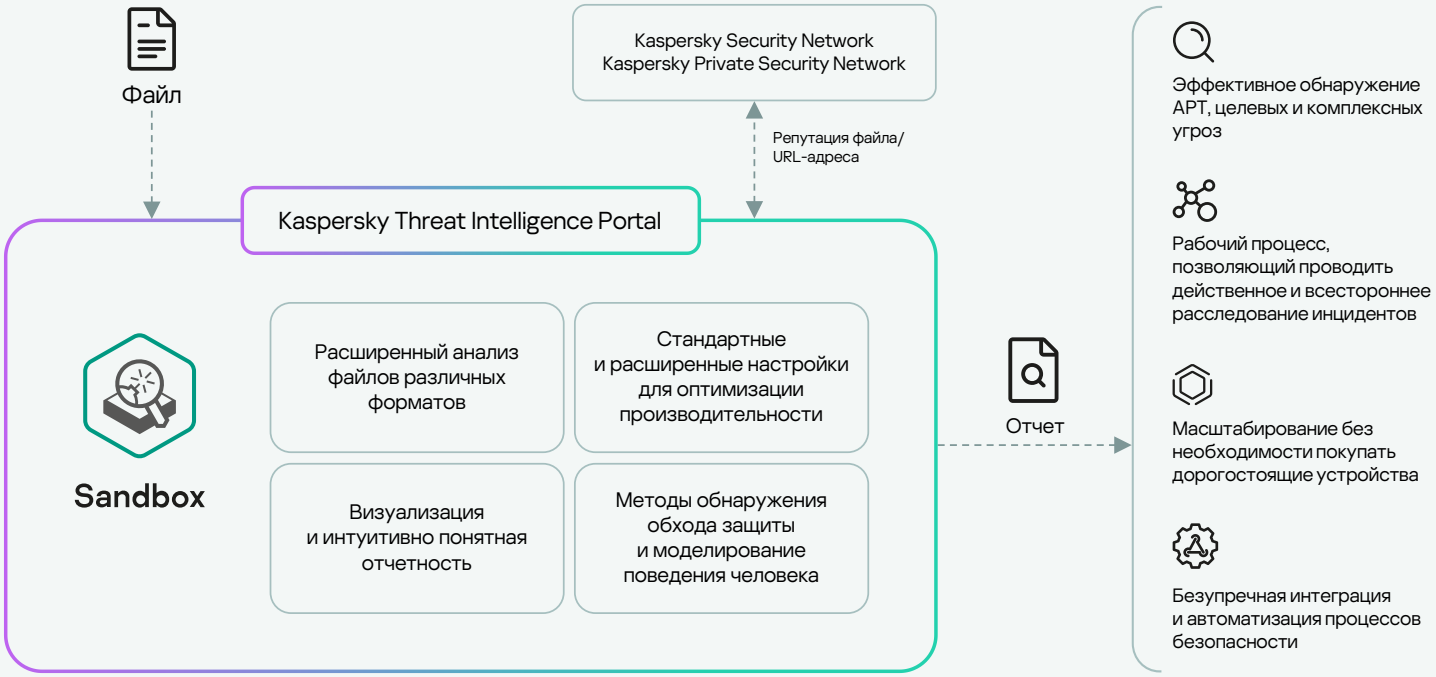
Особенности продукта

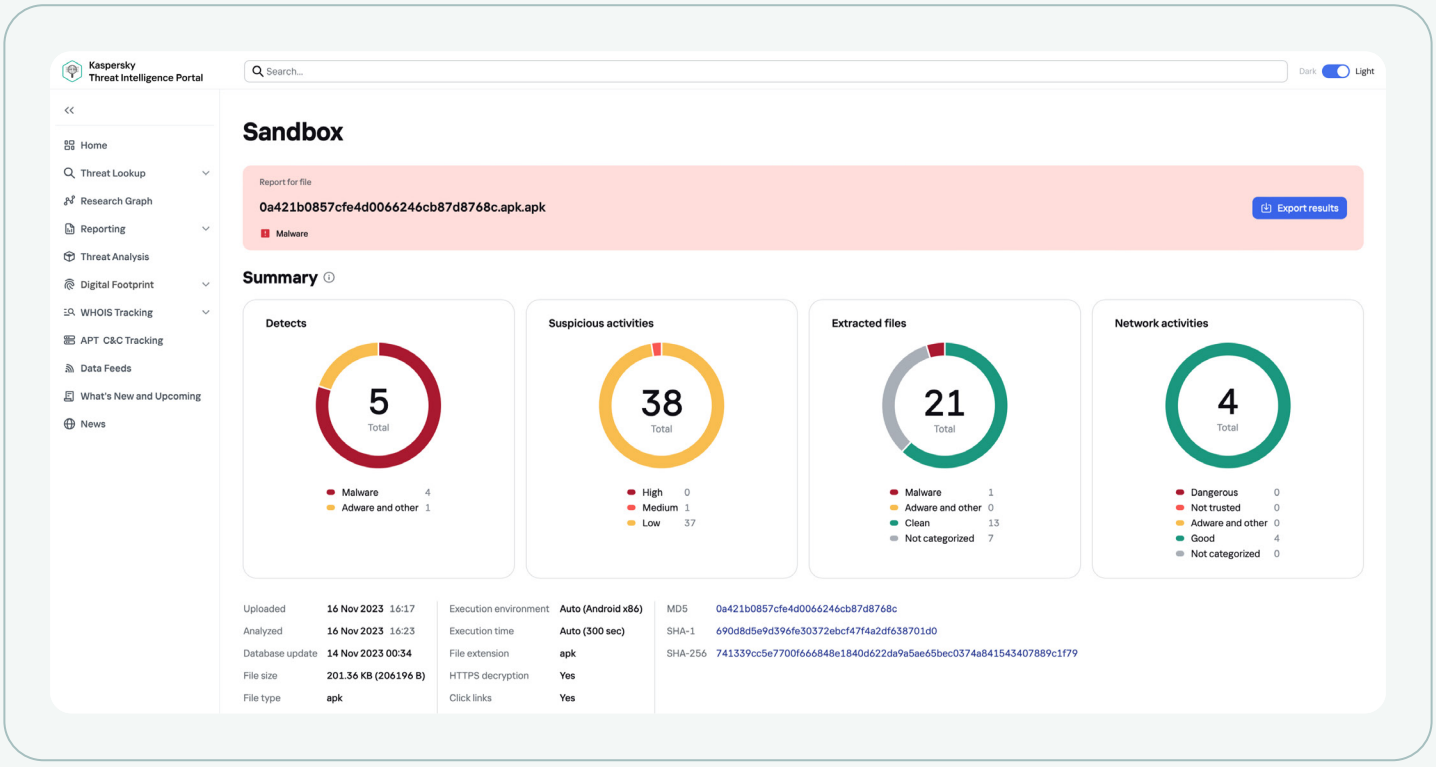
- Автоматизированный анализ объектов в средах Windows, Linux и Android
- Поддержка анализа более 200 типов файлов с подробными аналитическими отчетами
- Более 1000 правил классификации вредоносного поведения файла по тактикам и техникам MITRE ATT&CK
- Защита от уклонения вредоносных файлов от анализа и передовые технологии эмуляции активности пользователей
- Определение рейтинга угроз и уровня опасности анализируемого объекта по метрикам и данным, полученным в результате исполнения файла
- Возможность проверять сетевой трафик, генерируемый при выполнении файла, с помощью преднастроенных Suricata правил
- Отправка файлов на анализ вручную и посредством API

В основе Sandbox лежит запатентованная технология «Лаборатории Касперского» (№ патента US10339301). Песочница воссоздает условия для запуска вредоносного кода, позволяя исследователям анализировать подозрительный файл или URL-адрес.

Чтобы избежать разоблачения, вредоносный файл в процессе выполнения может пытаться определить, находится ли он в виртуальной среде, или оставаться неактивным в течение некоторого времени, пока песочница предположительно не завершит процесс анализа его выполнения. Запатентованная технология ускоряет течение времени на виртуальной машине, что позволяет инициировать выполнение вредоносного кода, не дожидаясь истечения запрограммированного в нем времени ожидания.

Схема работы Sandbox





Подробные аналитические отчеты

По завершении анализа Sandbox предоставляет подробный отчет о поведении анализируемого файла, позволяющий реализовать подходящие меры противодействия. Отчет содержит следующие сведения:

Краткие сведения	Общая информация о результатах выполнения файла или проверки URL адреса
Обнаруженные угрозы	Список угроз, выявленных в процессе выполнения файла стандартным антивирусом и технологиями поведенческого анализа
Сработавшие сетевые правила	Список сетевых Suricata-правил, сработавших во время анализа трафика от запущенного объекта
Карта выполнения файла	Графически представленные действия объекта и взаимосвязи между ними
Подозрительная активность	Список зарегистрированных подозрительных действий
Скриншоты	Набор скриншотов, сделанных во время выполнения файла или проверки URL-адреса
Загруженные PE-образы	Список загруженных PE-образов, обнаруженных во время выполнения файла или проверки URL-адреса
Файловые операции	Список файловых операций, которые были зарегистрированы во время выполнения файла или проверки URL-адреса
Операции с реестром	Список операций с реестром ОС, обнаруженных во время выполнения файла или проверки URL-адреса.
Операции с процессами	Список взаимодействий файла с различными процессами, которые были зарегистрированы во время выполнения файла.
Операции синхронизации	Список операций созданных объектов синхронизации (мьютекс, событие, семафор), которые были зарегистрированы во время выполнения файла или проверки URL-адреса
Загруженные файлы	Список файлов, извлеченных из сетевого трафика во время выполнения файла или проверки URL-адреса
Сохраненные файлы	Список файлов, которые были сохранены (созданы или изменены) выполняемым файлом
HTTPS/HTTP/DNS/IP/TCP/UDP и др.	Сведения о сетевых сеансах/запросах, зарегистрированных во время выполнения файла или проверки URL-адреса.
Дамп сетевого трафика (PCAP)	Сетевая активность, которая может быть экспортирована в формат PCAP
Матрица MITRE ATT&CK	Вся активность процессов, зафиксированная в ходе эмуляции, представлена в виде матрицы MITRE ATT&CK

Kaspersky
Threat Analysis

Attribution

Аналитический инструмент, помогающий определить возможных авторов и источник вредоносного ПО.

Технология основана на уникальном методе сравнения анализируемых экземпляров подозрительных файлов с целью выявления степени сходства с вредоносными образцами из коллекции «Лаборатории Касперского», обеспечивая практически нулевой процент ложноположительных срабатываний. Система атрибуции «Лаборатории Касперского» позволяет сопоставить новые потенциальные угрозы с известными хакерскими группировками.

Attribution

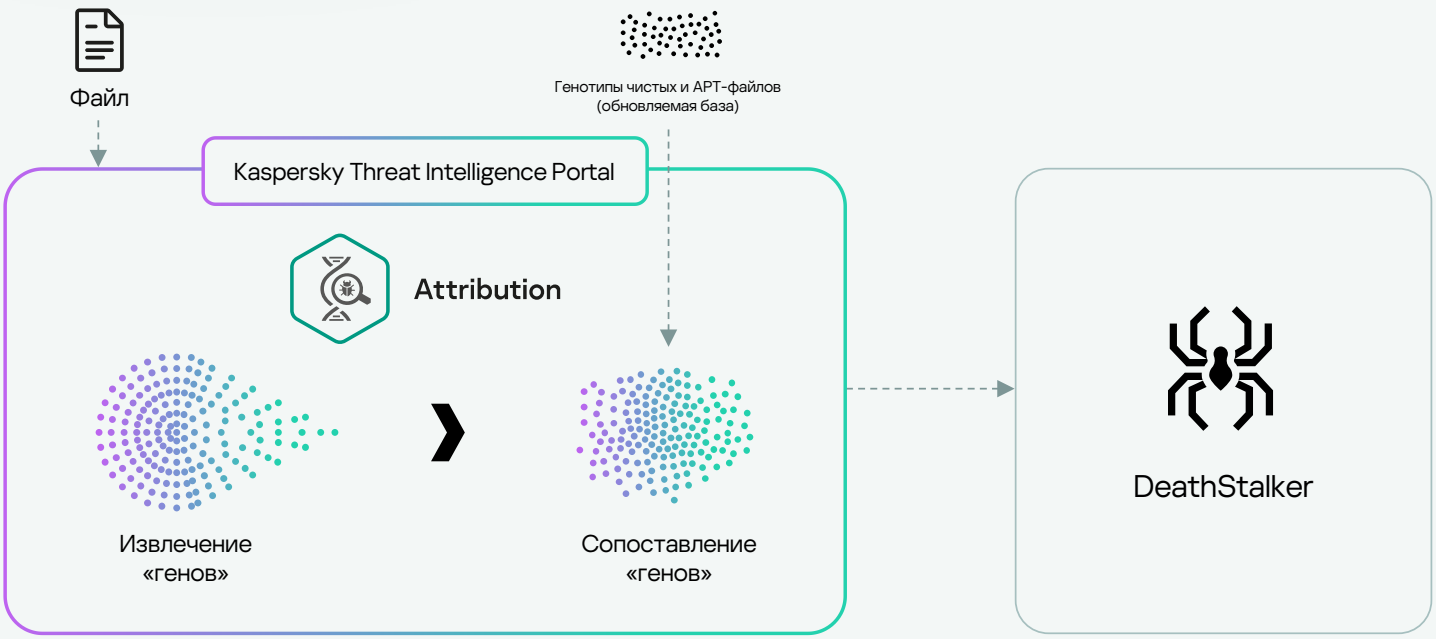
Как правило вредоносные программы, написанные одним и тем же автором, имеют общие паттерны. Сэмплы, оставленные злоумышленниками, тщательно анализируются. На основе уникального кода, обнаруженного во вредоносном файле можно найти похожие на него объекты. Эксперты «Лаборатории Касперского», обнаружившие десятки атак глобального масштаба за годы работы, постоянно изучают новые угрозы и проводят скрупулезные исследования APT-атак. Эти обширные знания легли в основу технологии Attribution, которая позволяет атрибутировать новую угрозу к ранее исследованному вредоносному ПО и APT-группировке.

«Лаборатория Касперского» отслеживает более 1100 угроз и кампаний и выпускает 200+ отчетов об угрозах ежегодно. Исследования экспертов непрерывно пополняют коллекцию APT-файлов, содержащую уже более 80 000 образцов, что в сочетании с использованием автоматизированных инструментов позволяет добиться исключительной точности атрибуции.

Какую проблему решает?

Атрибуция файла к определенной хакерской группировке наряду с информацией о том, как именно атакуют эти киберпреступники, дает возможность определить место и назначение данного файла в общей цепочке атаки. В свою очередь, это дает возможность предположить, где необходимо искать другие IoC/IoA, чтобы, заблокировав отдельный вредоносный файл, не пропустить основную атаку. Все это позволяет оперативно проводить анализ и принимать эффективные меры по защите от целевых атак.

Схема работы Attribution



Особенности продукта

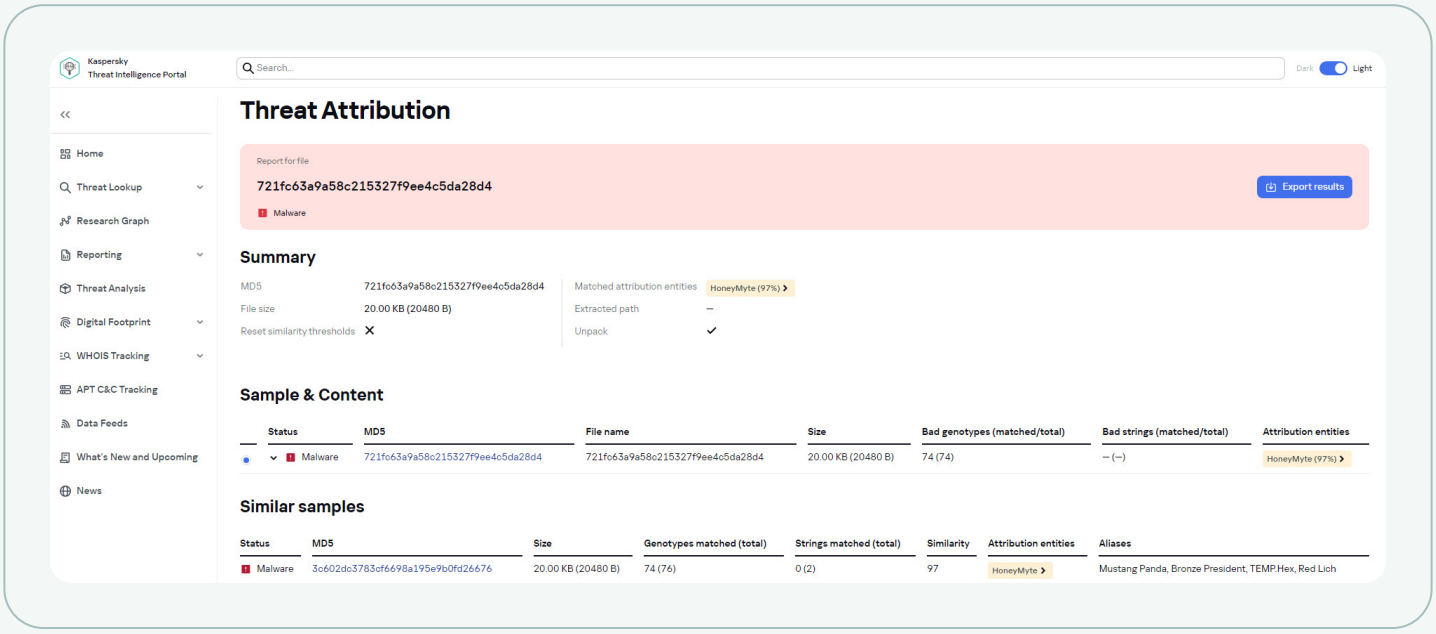
Мгновенный доступ к хранилищу, где содержатся коллекции данных о сотнях APT-компаний и множестве экземпляров вредоносного ПО

Экспорт YARA-правил для дальнейшего автоматизированного поиска похожих файлов в инфраструктуре

Загрузка экземпляров файлов через веб-интерфейс, а также по API (для интеграции с автоматизированными процессами)

Функциональность распаковки защищенных паролем архивов

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



Метод поиска сходства

Чтобы выявить связь подозрительных файлов с хакерскими группировками, Attribution использует уникальный запатентованный метод поиска сходства «генетического кода» файлов. Этот метод включает в себя:

Анализ генетики образца

путем извлечения из его кода следующих элементов:

- Генотипы — характерные фрагменты двоичного кода
- Строки — характерные строки символов

Автоматический поиск в анализируемых файлах

генотипов и строк, схожих с генотипами и строками образцов, встречавшихся в ранее расследованных APT-атаках или связанных с конкретными хакерскими группировками

На основе найденных схожих данных

формируется отчет о файлах, связанных с анализируемым образцом, и используемых конкретными хакерскими группировками

Kaspersky
Threat Analysis

Similarity

Инструмент для выявления файлов со схожей функциональностью, позволяющий защититься от неизвестных и скрытых угроз.

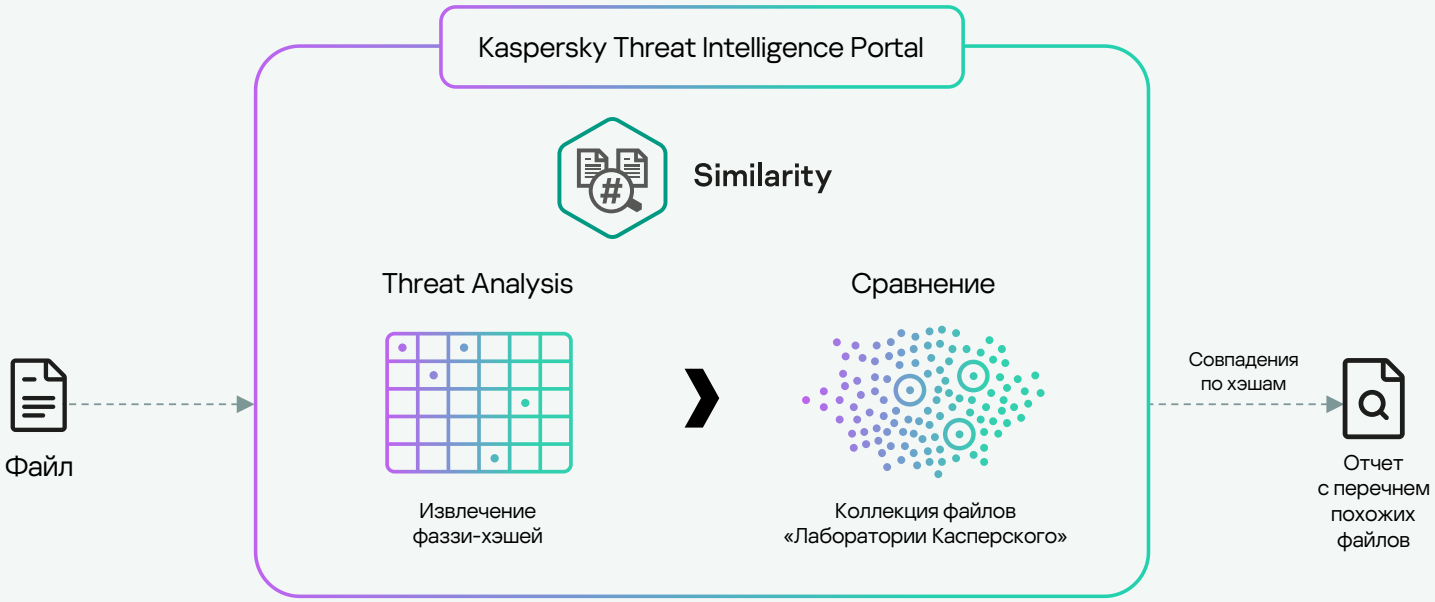
Similarity

Для выстраивания надежной линии обороны не обязательно знать врага в лицо. Similarity — удобный инструмент для выявления файлов, которые функционируют схожим образом, созданный на основе новейшей технологии, разработанной ведущими экспертами «Лабораторией Касперского». Для определения схожести используется более 50 уникальных типов специальных хэшей, а также база данных образцов вредоносного ПО, накопленная «Лабораторией Касперского» более, чем за 25 лет, и содержащая миллионы вредоносных файлов, что позволяет обеспечить высочайшую точность и достоверность результатов.

Какую проблему решает?

Технология позволяет находить в инфраструктуре файлы, похожие по своему поведению на уже известное «Лаборатории Касперского» вредоносное ПО (в том числе уклоняющееся от средств защиты). Благодаря уникальному методу определения схожести можно выявить даже те вредоносные файлы, которые не удалось связать с известными хакерскими группировками. Это дает уверенность в том, что любое изменение злоумышленником вредоносного файла с целью уклонения от обнаружения останется в поле вашего зрения.

Схема работы Similarity



Отчеты

Каждый файл имеет определенный формат, содержит специфические строки, секции, таблицы импорта, может использовать определенный набор программ-упаковщиков. Эксперты «Лаборатории Касперского» создали набор хэшей для определения схожести между файлами по данным признакам. При загрузке исследуемого файла на анализ в Similarity, система извлекает из него фаззи-хэши и сравнивает их с аналогичными хэшами вредоносных файлов, накопленных за более чем 25 лет в библиотеке образцов вредоносного ПО «Лаборатории Касперского». В случае обнаружения совпадений формируется список хэшей наиболее похожих на данный образец известных вредоносных файлов, отсортированных по степени схожести. В отчете содержится дополнительный контекст с метаданными для каждого похожего файла:

- Достоверность схожести
- Статус файла (вредоносное или рекламное ПО)
- Название угрозы (вердикт антивируса)
- Временные метки первого и последнего обнаружения
- Количество совпадений (обнаружений)
- Хэш файла
- Тип файла
- Размер файла

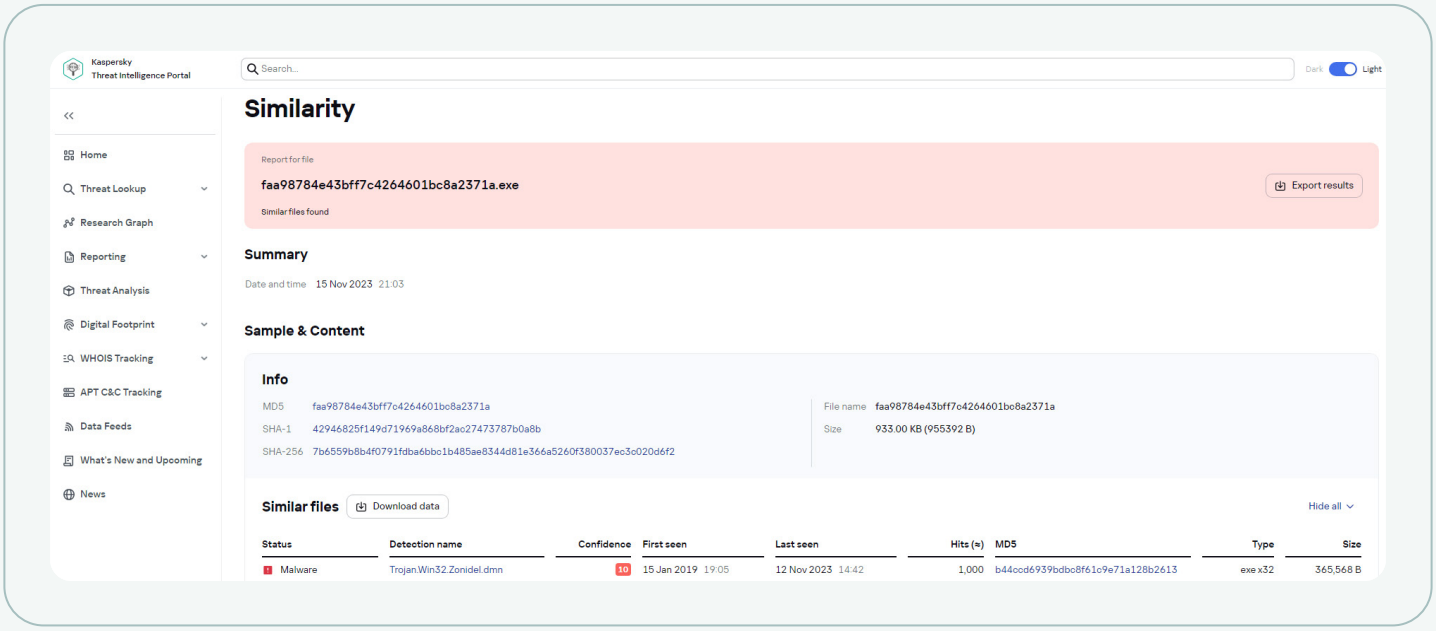
Особенности продукта

Для сравнения используется одна из самых крупнейших в отрасли коллекция данных вредоносных и чистых файлов – миллионы образцов, собранных ведущими экспертами «Лаборатории Касперского» более чем за 25 лет

Загрузка экземпляров файлов через веб-интерфейс и с использованием API (для интеграции с автоматизированными процессами)

Функциональность активно используется в том числе и экспертами «Лаборатории Касперского» для изучения новых угроз, с целью обеспечения максимального уровня защиты в наших продуктах, что регулярно подтверждается высокими оценками по результатам независимых тестов и обзоров

Подробнее



Сценарии использования Kaspersky Threat Analysis

Kaspersky Threat Analysis предоставляет собой полноценный набор инструментов для обнаружения киберугроз. Данные инструменты могут применяться в следующих сценариях:

Реагирование на инциденты

Обнаружение угроз, уклоняющихся от обнаружения средствами защиты

Статический/динамический анализ подозрительных файлов

Выявление связи нового вредоноса с определенной группировкой для понимания возможных дальнейших этапов атаки

Threat Hunting (активный поиск угроз)

Сканирование инфраструктуры на наличие IoCs, содержащихся в отчете

Поиск потенциально вредоносных модификаций популярных чистых файлов

Выявление общих IoCs между неизвестными и известными вредоносными файлами

Анализ вредоносного ПО

Анализ неизвестных угроз

Поиск и анализ схожих вредоносных файлов для определения функциональности исходных обфусцированных файлов

Kaspersky Threat Analysis — это гибкий и мощный инструментарий, состоящий из взаимосвязанных компонент, позволяющих проводить комплексный и многоуровневый анализ подозрительных файлов для выявления и классификации современных киберугроз. Данный инструментарий помогает командам SOC, исследователям безопасности и аналитикам вредоносного ПО оставаться в курсе существующих и возникающих угроз, позволяя быстро расставлять приоритеты и фокусироваться в первую очередь на устранении наиболее критических проблем безопасности.

Kaspersky Threat Analysis

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее