Kaspersky Threat Intelligence

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Задача

Наблюдать за эволюцией киберугроз, анализировать их, вовремя на них реагировать и сводить к минимуму их последствия – чрезвычайно трудоемкий процесс. Организации во всех отраслях сталкиваются с нехваткой достоверных и оперативно обновляемых данных об угрозах. Чтобы эффективно управлять рисками безопасности, необходимо регулярно получать такие данные.

Kaspersky Threat Intelligence

«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 включает:

Kaspersky Threat Data Feeds, Kaspersky CyberTrace, Kaspersky Threat Lookup, Kaspersky Cloud Sandbox, набор аналитических отчетов об угрозах и сервисы, по запросу предоставляющие экспертную информацию об угрозах.

Kaspersky Threat Data Feeds
Потоки данных об угрозах

Кибератаки происходят каждый день. Попытки взломать защиту предпринимаются все чаще, при этом сложность и скрытность киберугроз растет. Для кампаний, направленных на нарушение ваших бизнес-процессов и нанесение ущерба вашим клиентам, злоумышленники используют многоступенчатые атаки, а также специально подобранные тактику и методы. В этой ситуации необходимы новые методы защиты, основанные на анализе угроз.

Благодаря интеграции потоков данных об угрозах, содержащих подозрительные и вредоносные IP-адреса, веб-адреса и хеши файлов, с существующими системами безопасности, такими как SIEM, SOAR, и платформами Threat Intelligence службы информационной безопасности могут автоматизировать процесс приоритизации оповещений об угрозах. При этом специалисты по сортировке таких оповещений получают достаточно контекста, чтобы сразу выявлять события, требующие более пристального изучения или эскалации группам реагирования на инциденты для детального расследования.

Запрос пробного доступа к Kaspersky Threat Data Feeds

Подробнее

Контекстные данные

Каждая запись в каждом потоке содержит контекстные данные, позволяющие быстро подтвердить и приоритизировать угрозы (имена угроз, метки времени, географическое положение, установленные IP-адреса зараженных веб-ресурсов, хеши, популярность и прочее). Эти данные можно использовать, например, чтобы составить общее представление о событии или провести дополнительные проверки. Они помогут найти ответы на вопросы «кто?», «что?», «где?» и «когда?» и выявить источники атак, чтобы принимать своевременные решения и защищать компанию от угроз любой сложности.

Преимущества

Потоки данных генерируются автоматически в режиме реального времени на основе данных, собираемых по всему миру (в сеть Kaspersky Security Network входят десятки миллионов конечных пользователей более чем из 213 стран, что позволяет отслеживать значительный объем интернет-трафика). Это обеспечивает точность и высокую скорость обнаружения.

Простота внедрения. Для эффективной интеграции предоставляются дополнительная документация, образцы, помощь службы технической поддержки «Лаборатории Касперского».

В подготовке потоков данных участвуют сотни специалистов, включая аналитиков безопасности со всего мира, экспертов из глобального центра исследования и анализа угроз (GReAT) и ведущие команды отдела исследований и разработки (R&D). Специалисты по безопасности получают критически важную информацию и уведомления, генерируемые на основе надежных данных, не тратя время и силы на обработку некритичных оповещений.

Сбор и обработка данных

Данные собираются из множества разнообразных надежных источников, включая сеть Kaspersky Security Network и наши собственные поисковые роботы, сервис мониторинга ботнет-угроз (круглосуточное слежение за ботнетами, их целями и действиями), ловушки для спама, данные исследовательских групп и партнеров.

Вся собранная информация тщательно проверяется и очищается в режиме реального времени при помощи различных методов предварительной обработки: статистических критериев, песочниц, средств эвристического анализа, инструментов для определения сходств, профилирования моделей поведения и проверки аналитиками.

Простые форматы для распространения данных (JSON, CSV, OpenIoC, STIX) через HTTPS, TAXII и специализированные методы доставки позволяют с легкостью интегрировать потоки данных в ИБ-решения.

Все данные генерируются и отслеживаются мощной отказоустойчивой инфраструктурой, что обеспечивает постоянную доступность.

Потоки данных, содержащие много ложноположительных записей, практически бесполезны, поэтому проводятся скрупулезное тестирование и фильтрация данных, чтобы заказчикам предоставлялась только на 100% подтвержденная информация.

Ценность

Повышение эффективности решений для защиты сети, включая SIEM-системы, межсетевые экраны, системы обнаружения и предотвращения вторжений, прокси-серверы, решения для служб DNS и технологии противодействия APT-угрозам с помощью интеграции с постоянно обновляемыми потоками данных. Эти потоки данных содержат актуальные индикаторы компрометации с дополнительными контекстными данными, что позволяет вовремя обнаруживать кибератаки и лучше понимать намерения, возможности и цели злоумышленников. Поддерживаются ведущие SIEM-системы (HP ArcSight, IBM QRadar, Splunk и прочие) и платформы анализа угроз.

Ускорение реагирования на инциденты и расширение возможностей криминалистического анализа за счет автоматизации процесса первоначальной сортировки. Аналитики по безопасности получают контекстные данные для немедленного выявления предупреждений, подлежащих расследованию или передаче группам реагирования на инциденты.

Предотвращение утечки конфиденциальных данных и интеллектуальной собственности с зараженных устройств за пределы организации. Предотвращение утечки конфиденциальных данных и интеллектуальной собственности с зараженных устройств за пределы организации.

Поставщики управляемых услуг безопасности (MSSP) могут развивать свой бизнес, предлагая клиентам лучшую в отрасли аналитику угроз как услугу премиум-класса. Группы экстренного реагирования на инциденты (CERT) могут расширить свои возможности и повысить качество обнаружения и идентификации угроз.

Kaspersky CyberTrace Платформа для управления данными о киберугрозах

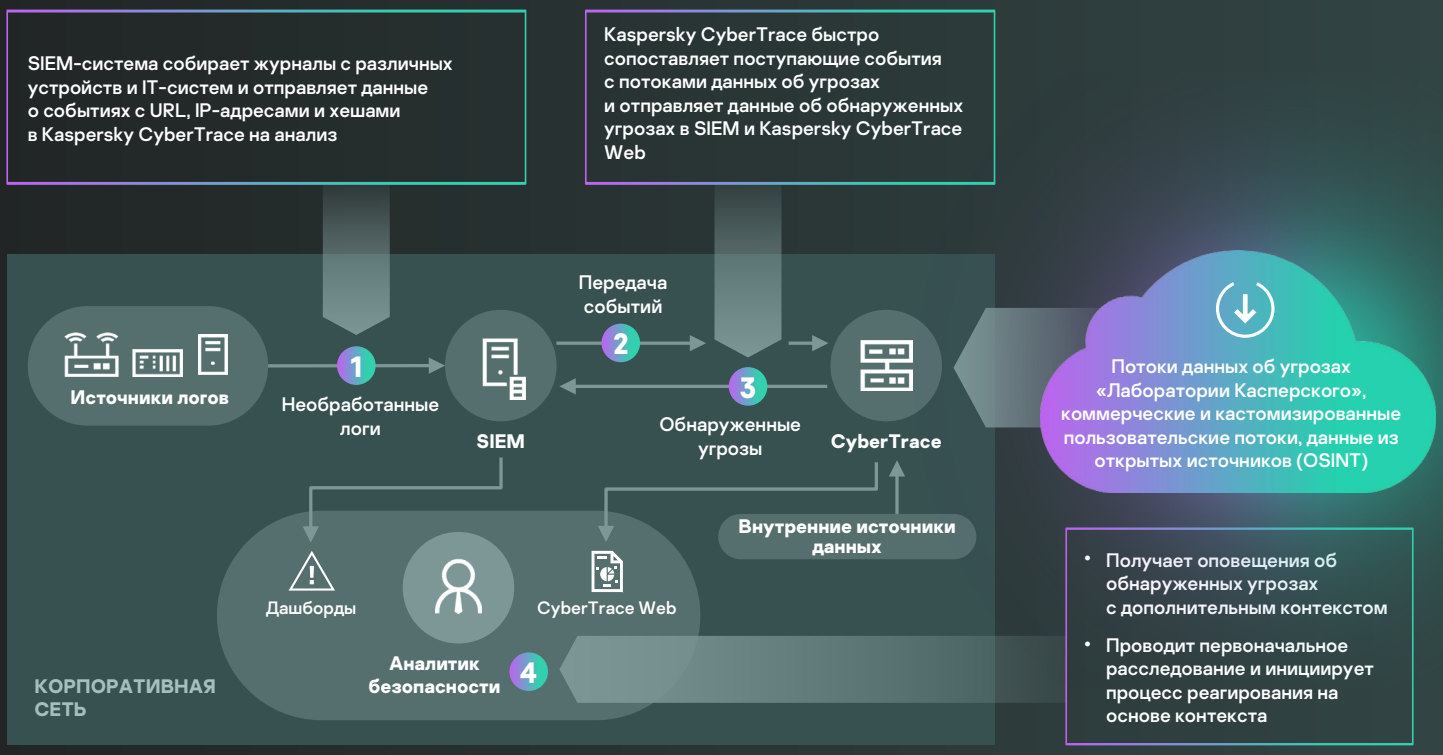
Интеграция актуальных машиночитаемых аналитических данных об угрозах в существующие средства управления безопасностью, такие как SIEM-системы, позволяет автоматизировать процесс первоначальной приоритизации и классификации. Но постоянный рост числа доступных для интеграции потоков данных об угрозах мешает определить источники информации, подходящие для конкретной организации. Аналитические данные предоставляются в различных форматах и включают большое количество индикаторов компрометации (IoCs), что сильно усложняет их обработку SIEM-системами или другими средствами управления сетевой безопасностью.

Kaspersky CyberTrace — это решение класса Threat Intelligence Platform, которое позволяет упростить интеграцию потоков данных с SIEM-системой для дальнейшего использования аналитики угроз в повседневной работе ИБ-служб. Платформа взаимодействует с любыми типами потоков аналитических данных об угрозах («Лаборатории Касперского», других поставщиков, из открытых источников или иных каналов) в форматах JSON, STIX, XML и CSV и поддерживает настроенную интеграцию со многими SIEM и источниками журналов. Благодаря автоматическому сопоставлению журналов с потоками аналитических данных об угрозах Kaspersky CyberTrace обеспечивает ситуационную осведомленность в реальном времени и позволяет аналитикам по безопасности принимать своевременные и взвешенные решения.

Kaspersky CyberTrace содержит набор инструментов для **эффективной классификации событий ИБ и первоначального реагирования**:

- База данных индикаторов с полнотекстовым поиском и возможностью поиска с использованием расширенных запросов позволяет выполнять сложный поиск по всем полям индикаторов.
- Страницы с подробной информацией о каждом индикаторе обеспечивают более глубокий анализ. Полная информация об индикаторе от всех поставщиков аналитических данных об угрозах (с исключением дублирующихся данных) позволяет аналитикам обсуждать угрозы в комментариях и добавлять внутренние данные к индикатору.
- Research Graph позволяет визуально изучать хранящиеся в CyberTrace сведения и обнаружения и выявлять общие черты угроз.
- Функция экспорта индикаторов позволяет экспортировать наборы индикаторов и передавать данные об угрозах между экземплярами Kaspersky CyberTrace или другими платформами анализа угроз.
- Назначение тегов индикаторам компрометации упрощает управление ими. Можно создать любой тег, указать его значимость и присваивать его индикаторам компрометации вручную. Можно выполнять сортировку и фильтрацию индикаторов по тегам и их значимости.
- Ретроспективная проверка позволяет анализировать объекты в ранее проверенных событиях с использованием последних потоков данных для поиска не обнаруженных ранее угроз.
- Фильтрация событий обнаружения для дальнейшей отправки в SIEM-системы снижает нагрузку как на сами системы, так и на аналитиков.
- Статистика использования потоков данных помогает выбрать наиболее ценных поставщиков аналитической информации об угрозах посредством измерения эффективности интегрированных потоков данных и построения матрицы пересечения потоков данных.
- Для поставщиков управляемых услуг безопасности, а также для использования на крупных предприятиях реализована поддержка мультитенантности.
- REST API позволяет выполнять поиск и управлять аналитическими данными об угрозах, а также интегрировать Kaspersky CyberTrace в сложные среды для автоматизации и управления.

Решение использует внутренний процесс анализа и сопоставления поступающих данных, что существенно снижает рабочую нагрузку на SIEM-систему. Kaspersky CyberTrace анализирует поступающие данные, быстро сопоставляет их с потоками и генерирует собственные оповещения при обнаружении угроз. На схеме ниже показана высокоуровневая архитектура решения.



Kaspersky CyberTrace и потоки данных «Лаборатории Касперского» об угрозах позволяют аналитикам безопасности:

- эффективно фильтровать и приоритизировать огромное количество оповещений систем безопасности;
- оптимизировать и ускорять процессы классификации и сдерживания угроз;
- быстро определять наиболее критичные из оповещений и принимать более взвешенные решения об их дальнейшей передаче группам реагирования;
- создавать проактивную систему защиты на основе глобальных аналитических данных.

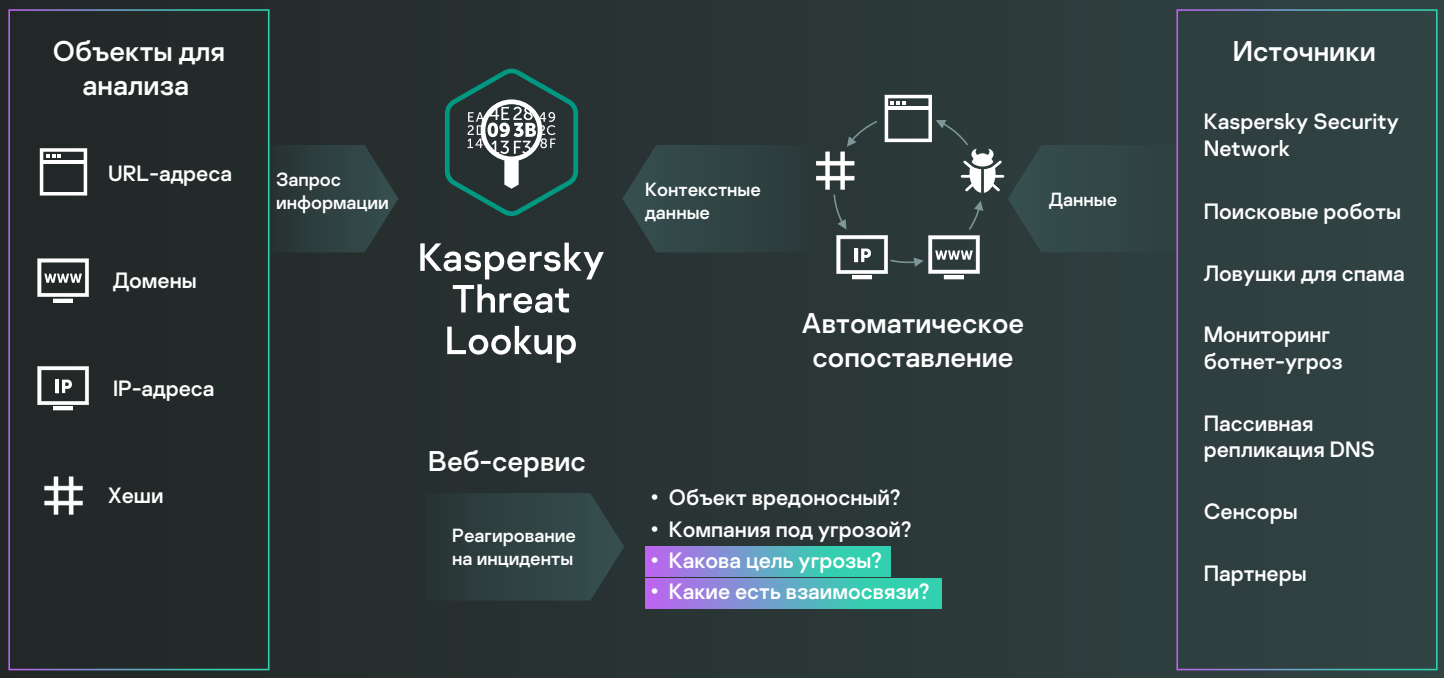
Kaspersky Threat Lookup
Поисковый портал о киберугрозах и их взаимосвязях

Киберпреступность не знает границ, а ее техническая база быстро совершенствуется. Попытки взломать защиту предпринимаются все чаще, при этом сложность и скрытность киберугроз растет. Для кампаний, направленных на нарушение рабочих процессов, кражу активов и нанесение ущерба, злоумышленники используют сложные цепочки поражения, а также специально подобранные тактики, техники и процедуры.

Kaspersky Threat Lookup – это мощная единая онлайн-платформа, открывающая доступ ко всем накопленным «Лабораторией Касперского» знаниям о киберугрозах и их взаимосвязях. Сервис предоставляет специалистам по безопасности максимум информации для предотвращения кибератак до того, как организации будет нанесен вред. Портал предоставляет самые последние данные по веб-адресам, доменам, IP-адресам, хешам файлов, названиям угроз, статистическим и поведенческим данным, данным WHOIS / DNS, атрибутам файлов, данным геолокации, цепочкам загрузки, временным меткам и прочему. Результатом является глобальная видимость новых и возникающих угроз, что помогает защитить организацию и ускоряет реагирование на инциденты.

Запрос пробного доступа к Kaspersky Threat Lookup

Подробнее



Преимущества

Надежные данные об угрозах: «Лаборатория Касперского» предоставляет надежные данные об угрозах детальной контекстной информацией. Продукты «Лаборатории Касперского» демонстрируют наилучшие результаты при тестировании решений для защиты от вредоносных программ. Непревзойденное качество аналитических данных подтверждается высоким уровнем обнаружения с минимальным уровнем ложных срабатываний.

Поиск угроз: проактивный подход к предотвращению и обнаружению атак и реагированию на них позволяет минимизировать частоту инцидентов и ущерб. Вы сможете отслеживать и устранять атаки на самых ранних этапах. Чем раньше будет обнаружена угроза, тем меньший будет нанесен ущерб и тем быстрее будет восстановлена работоспособность ресурсов и сети.

Расследование инцидентов: Research Graph ускоряет расследование инцидентов, позволяя визуально изучать хранящиеся в Threat Lookup данные и обнаружения; дает графическое представление связей между веб-адресами, доменами, IP-адресами, файлами и другими данными для иллюстрации полного масштаба инцидента и выявления его основной причины.

Мастер-поиск: поиск информации с использованием всех активных сервисов анализа угроз и внешних источников (включая индикаторы компрометации из открытых источников, а также поиск в теневом и поверхностном интернете) в едином и мощном интерфейсе.

Простота использования через веб-интерфейс или REST API: сервисом можно пользоваться в ручном режиме через веб-интерфейс (в браузере) или через REST API.

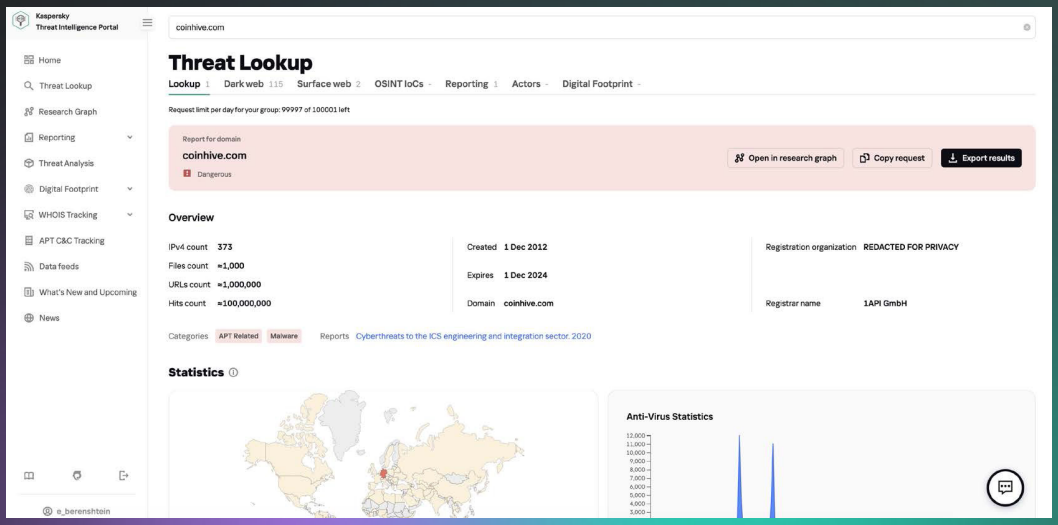
Разнообразие форматов экспорта: поддерживается экспорт индикаторов компрометации и контекстных данных в популярные машиночитаемые форматы, такие как STIX, OpenIOC, JSON, YARA, Snort и CSV. Это позволяет применять данные об угрозах с максимальной пользой, автоматизируя рабочие процессы и интегрируя эти сведения в системы управления безопасностью, такие как SIEM.

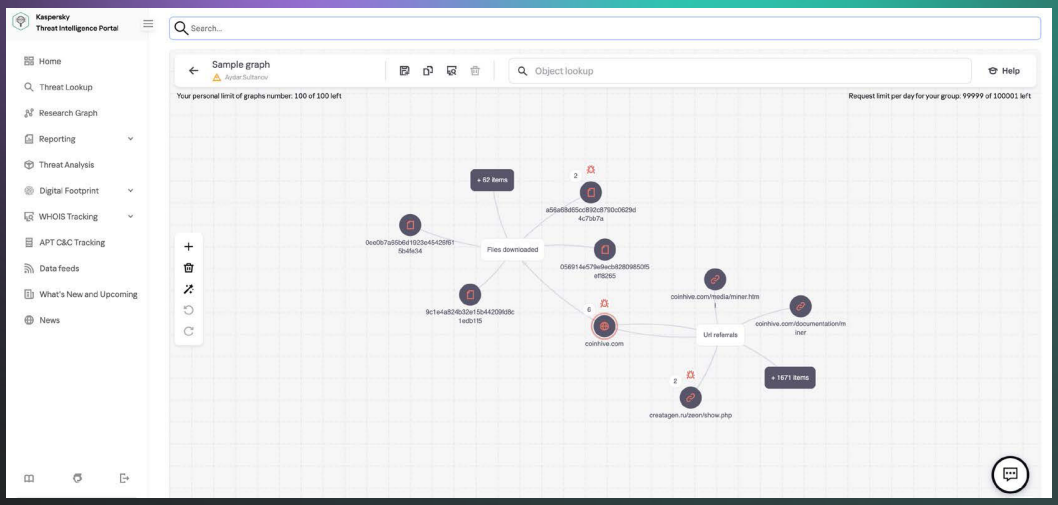
Ценность

Глубокий анализ индикаторов угроз с помощью проверенной контекстной информации позволяет приоритизировать атаки и сосредоточиться на устранении угроз, представляющих наибольший риск для бизнеса.

Эффективная и результативная диагностика и анализ инцидентов безопасности на узлах и в сети. Приоритизация сигналов о неизвестных угрозах от внутренних систем.

Улучшение процесса реагирования на инциденты и расширение возможностей поиска угроз, позволяющее прервать цепочку развития угрозы до момента компрометации критически важных систем и данных.





Платформа поможет:

Найти информацию об индикаторах угроз с помощью веб-интерфейса или REST API.

Выяснить, является ли обнаруженный объект распространенным или уникальным.

Понять, почему объект считается вредоносным.

Получить подробные сведения об объекте, включая сертификаты, распространенные названия, пути файлов и веб-адреса, для выявления новых подозрительных объектов.

Kaspersky Cloud Sandbox
Облачная песочница

Принятие аналитического решения на основе поведения файла при одновременном анализе памяти процессов, сетевой активности и прочих показателей – это оптимальный подход к пониманию современных комплексных целевых и APT-угроз.

Запрос пробного доступа к Kaspersky Cloud Sandbox

Подробнее

Современные целевые атаки невозможно предотвратить, используя только традиционные превентивные инструменты. Антивирусный движок способен останавливать только известные угрозы и их разновидности, в то время как создатели вредоносного ПО пускают в ход все средства, чтобы скрыть его от автоматического обнаружения. При этом убытки от киберинцидентов могут составлять десятки миллионов рублей, поэтому важно быстро обнаруживать угрозы и реагировать до нанесения ими серьезного ущерба.

В статистических данных часто не хватает информации о недавно измененных вредоносных программах. В то же время, технологии песочницы – это мощный инструмент, который позволяет исследовать исходные образцы файлов, находить индикаторы компрометации на основании поведенческого анализа и обнаруживать вредоносные объекты, которые не встречались ранее.

Веб-интерфейс

REST API

- Стандартные и расширенные настройки для оптимизации производительности
- Расширенный анализ файлов различных форматов
- Визуализация и интуитивно понятная отчетность
- Блокирование обхода механизмов обнаружения и моделирование активности пользователей

- Расширенное обнаружение APT-, целевых и сложных угроз
- Рабочий процесс, позволяющий проводить действенное и всестороннее расследование инцидентов
- Масштабирование без необходимости покупать дорогостоящие устройства
- Безупречная интеграция и автоматизация процессов безопасности

Проактивное выявление и предотвращение угроз

Комплексная отчетность:

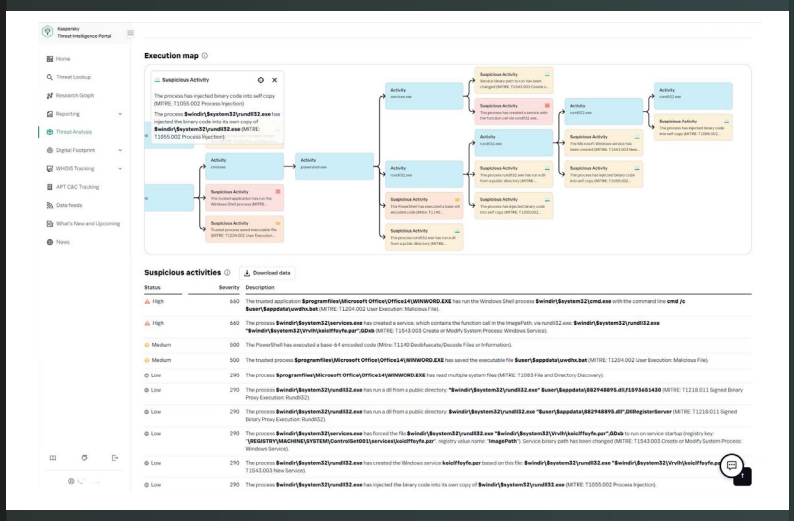
- Загрузка и запуск библиотек DLL
- Внешнее соединение с доменными именами и IP-адресами
- Создание, изменение и удаление файлов
- Подробная информация об угрозах с рекомендациями для каждого выявленного индикатора компрометации
- Дампы памяти процессов и сетевого трафика (PCAP)
- Запросы и ответы HTTP и DNS
- Создание взаимных исключений (мьютексы)
- REST API
- Изменение и создание ключей реестра
- Создание процессов с помощью выполняемого файла
- Снимки экрана
- И многое другое

При выполнении вредоносных программ используются различные методы обхода механизмов обнаружения. Если система жертвы не отвечает определенным критериям, вредоносная программа самоуничтожится, не оставив следов. Для выявления вредоносного кода песочница должна уметь точно имитировать поведение обычного пользователя.

В изолированной среде проводится поведенческий анализ и используются надежные механизмы блокировки таких методов. Также песочница применяет технологии моделирования поведения человека, такие как автокликер, прокрутка документов, и другие действия.

Облачная песочница «Лаборатории Касперского» объединяет все знания о поведении вредоносных программ, полученные за более чем 20 лет непрерывного исследования угроз, что позволяет обнаруживать более 380 000 новых вредоносных объектов каждый день.

Kaspersky Cloud Sandbox является важным компонентом для анализа угроз. В рамках сервиса Kaspersky Threat Lookup собираются подробные актуальные сведения об угрозах: веб-адреса, домены, IP-адреса, хеши файлов, названия угроз, статистические и поведенческие данные, данные WHOIS/DNS и прочие. Облачная песочница позволяет связать эти данные с индикаторами компрометации, сгенерированными анализируемым образцом.



Благодаря Kaspersky Cloud Sandbox можно провести высокоэффективное сложное расследование инцидентов, сразу понять характер угрозы и благодаря интеграции с сервисом Kaspersky Threat Lookup объединить собранные в ходе расследования данные в общую картину, выявляя взаимосвязанные индикаторы угрозы.

Облачная песочница сокращает время реагирования на инциденты и повышает эффективность криминалистического расследования, обеспечивая масштабируемость при автоматической обработке файлов без необходимости и беспокоиться о системных ресурсах.

Аналитические отчеты об APT-угрозах

Получатели аналитических отчетов об APT-угрозах имеют уникальный постоянный доступ к исследованиям и открытиям «Лаборатории Касперского», включая полные технические данные (в различных форматах) о каждой обнаруженной APT. Отчеты содержат ориентированную на руководство и легкую для понимания информацию, описывающую APT-угрозы, а также подробные технические данные об APT-угрозах с соответствующими индикаторами компрометации и правилами YARA, чтобы предоставить исследователям безопасности, аналитикам вредоносных программ, инженерам по безопасности и другим ИБ-аналитикам данные, позволяющие быстро и точно отреагировать на угрозу.

Специалисты «Лаборатории Касперского» также немедленно сообщают обо всех обнаруженных изменениях в тактиках киберпреступных групп. У вас также будет доступ к полной базе данных отчетов об APT-угрозах – еще одному мощному компоненту исследования и анализа.

Узнать больше о Kaspersky APT Intelligence Reporting

Подробнее

Преимущества

MITRE ATT&CK

Все тактики и техники злоумышленников, описанные в отчетах, сопоставляются с базой данных MITRE ATT&CK. Это позволяет улучшить качество обнаружения и реагирования на соответствующие тактики и техники злоумышленников.

Информация о непубличных APT-угрозах

По разным причинам не все громкие угрозы становятся известны широкой публике. Но мы предоставляем такую информацию нашим клиентам.

Эксклюзивные данные

Доступ к техническим описаниям новейших угроз уже в ходе расследования, до публичного объявления.

Ретроспективный анализ

В течение срока действия подписки доступны все ранее выпущенные закрытые отчеты.

Доступ к техническим данным

Технические данные включают расширенный список индикаторов компрометации, доступный в стандартных форматах, таких как openIOC и STIX, а также доступ к правилам YARA.

Профили злоумышленников

Профили злоумышленников включают предполагаемую страну происхождения, основной вид деятельности, используемые семейства вредоносных программ, целевые отрасли и географические регионы, а также описания всех используемых тактик и техник и их сопоставление с MITRE ATT&CK.

Непрерывный мониторинг APT-кампаний

Доступ к оперативной информации о распространении APT-угроз, индикаторах компрометации, инфраструктурах управления и контроля и прочих данных.

Поддержка RESTful API

Беспрепятственная интеграция и автоматизация процессов безопасности.

Развитие угроз

Угрозы категории crimeware постоянно меняются. Это вредоносные программы, созданные специально для совершения финансовых киберпреступлений. Программы-вымогатели, которые блокируют доступ к данным или снижают производительность устройства, – самый яркий пример. Фантазия злоумышленников безгранична: они изобретают все более изощренные способы получения доступа к системам, учетным записям и данным для извлечения финансовой выгоды.

Kaspersky Crimeware Intelligence Reporting

Киберпреступники, нацеленные на получение финансовой выгоды, действуют в разных отраслях и не ограничиваются атаками на банкоматы и платежные терминалы. Программы-вымогатели могут угрожать любой компании, чем бы она ни занималась. За последние пару лет границы между различными типами угроз и профилями киберпреступников размылись. Распространились APT-атаки, направленные не на кибершпионаж, а на кражу денег для финансирования различных преступлений. Не стоит недооценивать растущую сложность crimeware-угроз.

Kaspersky Crimeware Intelligence Reporting предлагает актуальную информацию о вредоносных кампаниях, атаках на финансовые организации и инструментах, нацеленных на банки, платежные компании и их инфраструктуру. Это помогает предприятиям лучше защищать свои активы от злоумышленников.

В состав сервиса входят:

Подробные описания самых известных и распространенных вредоносных программ

Сведения об опасных широкомасштабных вредоносных кампаниях

Наблюдения экспертов и ранние оповещения, в том числе о новом и обновленном вредоносном ПО

Подробное описание возможных атак на финансовые инфраструктуры и соответствующих инструментов, которые разрабатываются киберпреступниками и продаются через теневой интернет в разных странах

Преимущества сервиса

Профили киберпреступников, использующих ПО категории crimeware. Эти данные включают предполагаемую страну происхождения, основной вид деятельности, используемые семейства вредоносных программ, отрасли и регионы, на которые нацелены атаки, а также описания всех используемых тактик и методов, сопоставленных с базой данных MITRE ATT&CK.

Ретроспективный анализ. В течение срока действия подписки сохраняется доступ ко всем ранее выпущенным закрытым отчетам.

Привилегированный доступ. В рамках привилегированного доступа предоставляются технические описания угроз, обнаруженных в ходе текущих расследований, до того как они попадают в публичный доступ.

Технические данные, в том числе расширенный список индикаторов компрометации в стандартных форматах, таких как openIOC и STIX, а также доступ к YARA-правилам.

API на основе REST. Полная интеграция и автоматизация процессов безопасности.

Инструменты для атаки на финансовые организации

Наблюдения экспертов/ ранние предупреждения

Описания вредоносных программ

Вредоносные кампании

Kaspersky Crimeware Intelligence Reporting

Пробный доступ

Отчеты об угрозах для АСУ ТП

В рамках отчетов об угрозах для АСУ ТП «Лаборатория Касперского» предоставляет подробные аналитические данные о вредоносных кампаниях, нацеленных на промышленные организации, и об уязвимостях, обнаруженных в наиболее популярных АСУ ТП и их технологиях. Поскольку отчеты размещаются на интернет-портале, достаточно зарегистрироваться в сервисе, чтобы получить к ним доступ.

Что входит в сервис?

Отчеты об APT-атаках. Отчеты о новых APT-атаках и масштабных кампаниях против промышленных организаций и обновленные данные об активных угрозах.

Обнаруженные уязвимости. Отчеты об уязвимостях, обнаруженных «Лабораторией Касперского» в наиболее популярных продуктах для АСУ ТП, промышленном интернете вещей и IT-инфраструктуре различных отраслей.

Ландшафт угроз. Отчеты о значительных изменениях в ландшафте угроз для АСУ ТП и новых критических факторах, которые влияют на уровень безопасности и уязвимости таких систем, с разделением по регионам, странам и отраслям.

Анализ и минимизация уязвимостей. Эксперты «Лаборатории Касперского» дают практические рекомендации по выявлению и минимизации уязвимостей в инфраструктуре предприятия.

Данные анализа угроз позволяют

Выявлять и предотвращать

угрозы для критически важных устройств, включая программное и аппаратное обеспечение, чтобы обеспечить безопасность и непрерывность производственного процесса.

Сопоставлять

вредоносную и подозрительную активность, обнаруженную в промышленной среде, с результатами исследований «Лаборатории Касперского», чтобы связать эту активность с вредоносными кампаниями, определить угрозы и оперативно отреагировать на них.

Оценивать

уязвимости производственной среды и устройств на основе точных сведений о масштабах и серьезности обнаруженных проблем и принимать обоснованные решения по установке исправлений и другим рекомендованным профилактическим мерам.

Использовать

Информацию о тактиках, техниках и процедурах атак, недавно обнаруженных уязвимостях и других важных изменениях ландшафта угроз, чтобы:

- выявлять и оценивать риски, связанные с обнаруженными угрозами и их аналогами;
- планировать и внедрять изменения в производственную инфраструктуру для обеспечения безопасности и непрерывности производственного процесса;
- повышать осведомленность сотрудников о киберугрозах, разрабатывая тренинги с участием red team и blue team на основе анализа реальных случаев;
- принимать обоснованные стратегические решения об инвестициях в кибербезопасность и прочих мерах, повышающих защищенность процессов.

Kaspersky Digital Footprint Intelligence

Аналитические отчеты об угрозах для организации

По мере развития компании ее IT-инфраструктура становится все более сложной, поэтому появляется важная задача — защитить распределенные цифровые ресурсы, не имея прямого контроля над ними. Динамические и взаимосвязанные среды дают организациям множество преимуществ. Однако постоянный рост взаимосвязей расширяет поверхность атаки. Злоумышленники действуют все более изощренно, поэтому важно не только иметь точное представление об онлайн-присутствии предприятия, но также отслеживать изменения и реагировать на актуальные данные об уязвимых цифровых активах.

Компаниям доступно множество защитных инструментов, однако некоторые задачи по-прежнему вызывают у них трудности, например отслеживание киберпреступных планов и мошеннических схем на форумах даркнета. Чтобы аналитики по безопасности могли оценивать угрозы со стороны внешних атакующих, быстро выявлять возможные векторы атак и принимать стратегические решения по защите от них, «Лаборатория Касперского» разработала сервис Kaspersky Digital Footprint Intelligence.

Как лучше всего организовать атаку на вашу организацию? Как провести ее с наименьшими затратами? Какие сведения доступны злоумышленнику, решившему атаковать вашу компанию? Возможно, ваша инфраструктура уже взломана без вашего ведома?

Kaspersky Digital Footprint Intelligence отвечает на эти и другие вопросы. Эксперты «Лаборатории Касперского» формируют полную картину текущей ситуации с угрозами, выявляют уязвимости в защите и признаки прошедших, текущих и даже планируемых атак.

Возможности сервиса Kaspersky Digital Footprint Intelligence

- Сбор информации о ресурсах сетевого периметра и их уязвимостях с использованием полупассивных методов, чтобы определить потенциальные точки входа злоумышленников: доступные интерфейсы удаленного управления, неправильно сконфигурированные сервисы, интерфейсы сетевых устройств, службы, использующие устаревшие уязвимые версии ПО, и т.д.
- Выявление, мониторинг и анализ угроз, связанных с активностью вредоносных программ, APT-кампаний, которые могут быть нацелены на организацию, отрасль или регион.
- Выявление, мониторинг и анализ угроз в отношении клиентов компании, связанных с активностью ботнет-сетей, фишинговыми атаками и утечками чувствительных данных.
- Анализ активности киберпреступников на ресурсах даркнета (форумах, каналах обмена мгновенными сообщениями, onion-ресурсах и т.д.) для выявления скомпрометированных учетных записей сотрудников, продажи данных или обсуждений атак на организацию.

Преимущества

Персонализированные отчеты составляются на основе данных, полученных в результате автоматического и ручного анализа интернета, даркнета и глубокой сети, а также внутренней базы знаний «Лаборатории Касперского». Они содержат аналитические данные и рекомендации, которые позволяют сократить количество потенциальных векторов атаки и риски информационной безопасности для организации.

Сервис может включать четыре квартальных отчета с оповещениями об угрозах в Threat Intelligence Portal сроком на один год или разовый отчет об угрозах с оповещениями, активными в течение шести месяцев.

Сервис также предлагает свободный поиск по данным, полученным с ресурсов даркнета и тематических ресурсов по информационной безопасности. Годовая подписка на сервис включает до 50 поисковых запросов в день.

Анализ ресурсов сетевого периметра (включая облачные активы)

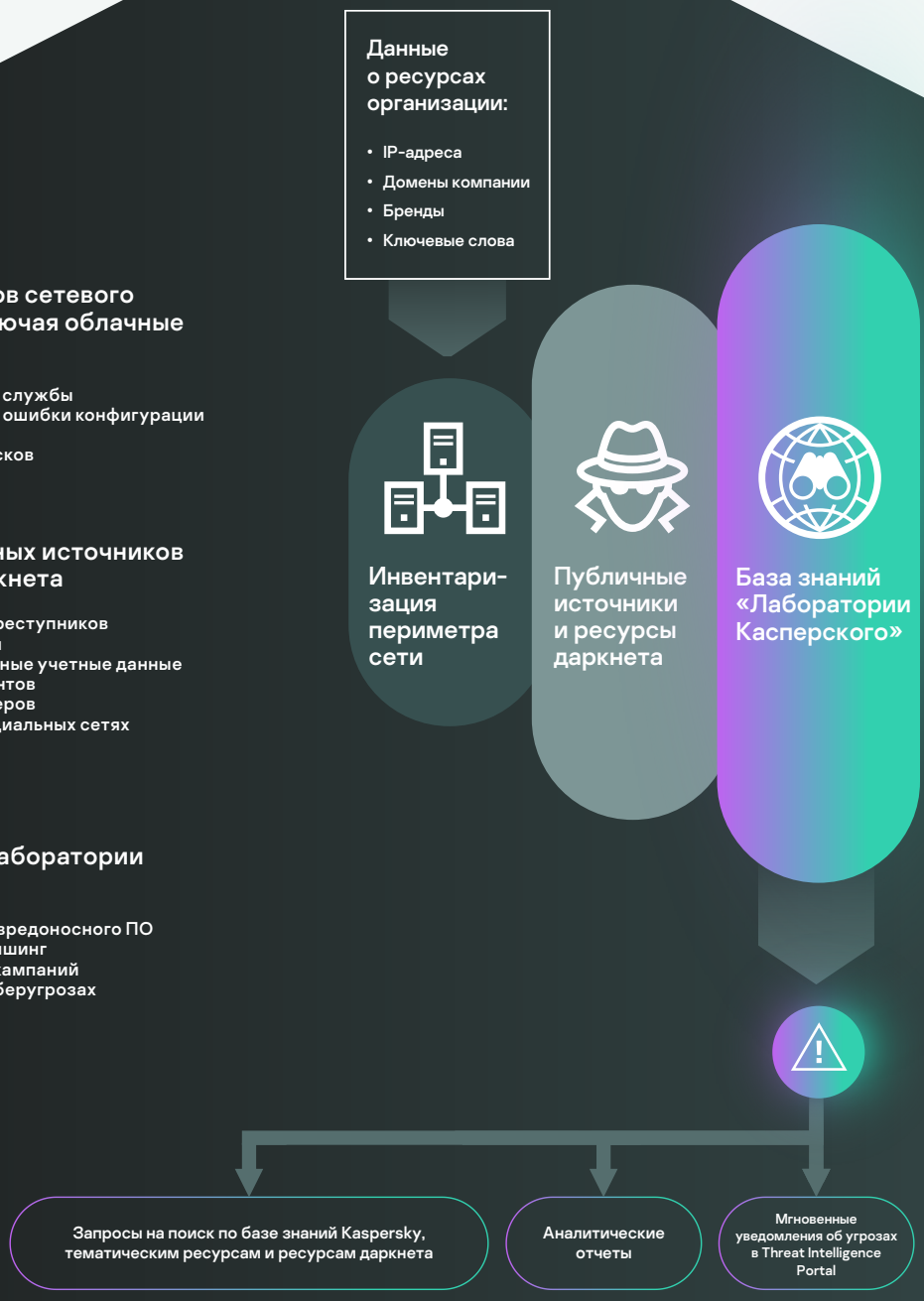
- Доступные сетевые службы
- Уязвимые службы и ошибки конфигурации
- Анализ эксплойтов
- Оценка и анализ рисков

Анализ публичных источников и ресурсов даркнета

- Активность киберпреступников
- Утечки информации
- Скомпрометированные учетные данные сотрудников и клиентов
- Активность инсайдеров
- Утечки данных в социальных сетях
- Утечки метаданных

База знаний «Лаборатории Касперского»

- Анализ активности вредоносного ПО
- Атаки ботнетов и фишинг
- Анализ жертв APT-кампаний
- Потоки данных о киберугрозах



Сервис Kaspersky Takedown

Преимущества сервиса

Глобальный охват

Где бы ни был зарегистрирован домен вредоносного или фишингового сайта, мы направим запрос на блокирование такого домена в организацию с необходимыми полномочиями в регионе.

Экономия ваших ресурсов

Мы позаботимся обо всем процессе блокирования – ваше участие в нем будет минимальным.

Полная прозрачность

Вы будете получать уведомления на каждом этапе процесса – от регистрации вашего запроса на блокирование до его исполнения.

Интеграция с сервисом Kaspersky Digital Footprint Intelligence

Решение интегрируется с сервисом Kaspersky Digital Footprint Intelligence, который в режиме реального времени оповещает о фишинговых и вредоносных сайтах, способных нанести вред вашей компании, спекулируя на вашем бренде или публикуя информацию от вашего имени. Единое решение — важный компонент комплексной стратегии кибербезопасности.

Почему это важно

Киберпреступники создают вредоносные и фишинговые домены для атак на организации и их бренды. Такие угрозы требуют немедленного реагирования, поскольку могут причинить финансовый ущерб, повредить репутации, привести к потере клиентов, утечке данных и другим неприятным последствиям. Однако блокирование доменов – комплексный процесс, которым должны заниматься эксперты.

Решение

За день «Лаборатория Касперского» блокирует более 15 000 фишинговых и мошеннических адресов и предотвращает более миллиона попыток перехода по таким ссылкам. За годы нашей работы мы проанализировали большое количество вредоносных и фишинговых доменов и знаем, как собирать доказательства их вредоносности. Мы возьмем на себя управление всем процессом блокировки и примем оперативные меры для снижения цифровых рисков для вашей компании, а вы сможете заняться другими приоритетными задачами.

«Лаборатория Касперского» предлагает своим клиентам эффективные решения для защиты онлайн-сервисов и репутации. Мы сотрудничаем с международными организациями, государственными и региональными правоохранительными органами (например, с Интерполом, Европолом, Национальным подразделением по борьбе с преступлениями в сфере высоких технологий (NHTCU) полицейского управления Нидерландов и полицией Лондона), а также с группами экстренного реагирования на инциденты (CERT) по всему миру.

Как это работает?

Запросы можно отправлять через свою корпоративную учетную запись на нашем портале поддержки корпоративных клиентов. Мы подготовим всю необходимую документацию и направим запрос на блокирование в компетентный местный или региональный орган (CERT, регистратор и т. д.), уполномоченный на исполнение такого запроса. Вы будете получать уведомления на каждом этапе работы с вашим запросом – до тех пор, пока домен не будет заблокирован.

Защита репутации

Сервис Kaspersky Takedown быстро нейтрализует угрозы, которые связаны с вредоносными и фишинговыми доменами, не позволяя им причинить вред вашей репутации и бизнесу. Мы обеспечим комплексное управление процессом, а вы сэкономите время и ресурсы.

«Лаборатория Касперского» постоянно исследует угрозы,

находит закрытые сообщества киберпреступников и форумы даркнета по всему миру, проникает в них и отслеживает активность злоумышленников. Наши аналитики пользуются доступом к этим ресурсам, чтобы проактивно находить и исследовать наиболее опасные угрозы, а также угрозы, направленные против конкретных организаций.

Ask the Analyst

Всегда на связи с лучшими экспертами

Ландшафт угроз непрерывно меняется, их количество быстро растет, а у злоумышленников появляются все более изощренные методы и техники для проведения атак. Все чаще происходят сложные киберинциденты, вызванные атаками без использования вредоносных программ, бесфайловыми атаками, атаками с использованием легитимных инструментов, эксплойтами «нулевого дня», а также встречаются различные комбинации этих сценариев, которые применяются для проведения сложных, целевых и APT-атак.

Кибератаки могут разрушить бизнес, поэтому профессионалы в области кибербезопасности важны как никогда. Но найти и удержать их бывает непросто. Даже если у вас есть компетентная ИБ-команда, ваши эксперты не всегда могут противостоять изощренным угрозам самостоятельно – **иногда им требуется обратиться к сторонним специалистам за помощью.** Привлекая внешних экспертов, вы сможете выявить наиболее вероятные векторы сложных и целевых атак и получить практические рекомендации по эффективной борьбе с ними.

Что дает сервис Ask the Analyst

Kaspersky Ask the Analyst дополняет наш портфель сервисов Kaspersky Threat Intelligence. С помощью этого сервиса вы можете обращаться к экспертам за поддержкой и полезной информацией по конкретным угрозам, с которыми вы сталкиваетесь или которые вас интересуют. Сервис персонализирует мощные инструменты аналитики угроз и проведения исследований «Лаборатории Касперского» под ваши потребности. Используя эти данные, вы сможете усовершенствовать систему защиты против угроз, нацеленных на вашу организацию.

Информация об APT-атаках и Crimeware-угрозах

Дополнительная информация об опубликованных ранее отчетах и текущих исследованиях; в дополнение к отчетам об APT-атаках и атаках с использованием специального ПО, разработанного для совершения преступлений (Crimeware)[1]

Описание угроз, уязвимостей и связанных с ними индикаторов компрометации

- Общее описание конкретных семейств вредоносного ПО
- Дополнительный контекст для индикаторов компрометации (связанные хеши, URL, командные серверы и т. д.)
- Информация о конкретных уязвимостях (насколько они критичны, какие механизмы продуктов «Лаборатории Касперского» защищают от них)

Анализ вредоносного ПО

- Анализ образцов вредоносного ПО
- Рекомендации по противодействию и устранению последствий

Анализ угроз в даркнете[2]

- Исследование даркнета на предмет конкретных артефактов, IP-адресов, доменных имен, имен файлов, адресов электронной почты, ссылок или изображений
- Поиск и анализ информации

Запросы, связанные с АСУ ТП

- Дополнительная информация об опубликованных отчетах
- Информация об уязвимостях АСУ ТП
- Статистика угроз АСУ ТП и новые тенденции по регионам и отраслям
- Анализ вредоносных программ, нацеленных на АСУ ТП
- Информация, касающаяся нормативных требований и стандартов

[1] Доступно только клиентам, которые подписались на отчеты об APT-атаках и (или) атаках с использованием Crimeware

[2] Уже включено в подписку Kaspersky Digital Footprint Intelligence

Преимущества сервиса

Заручитесь поддержкой профессионалов

Вы сможете при необходимости обращаться к отраслевым экспертам: вам больше не понадобится искать людей и нанимать в штат узких специалистов

Ускорьте расследование

Эффективно оценивайте инциденты безопасности и назначайте им приоритеты на основании персонализированной и подробной контекстной информации

Реагируйте быстро и точно

Оперативно реагируйте на угрозы и уязвимости, блокируя известные векторы атак с помощью инструкций наших экспертов

Как это работает

Подписку на сервис Kaspersky Ask the Analyst можно приобрести отдельно или в дополнение к любому другому нашему сервису Kaspersky Threat Intelligence.

Запросы в рамках сервиса можно отправлять через свою корпоративную учетную запись на нашем портале поддержки корпоративных клиентов. Мы направим ответ по электронной почте, но в случае необходимости и по согласованию с вами мы можем также организовать конференц-связь и (или) звонок с совместным доступом к экрану. После принятия вашего запроса мы сообщим вам предварительные сроки его обработки.

Примеры использования сервиса:

- Уточнение информации из ранее опубликованных отчетов об угрозах
- Получение дополнительной информации по уже обнаруженным индикаторам компрометации
- Получение подробного описания уязвимостей и рекомендации по защите от их эксплуатации
- Получение сведений об интересующей вас активности на ресурсах даркнета
- Получение общего отчета по семейству вредоносного ПО, включая его поведение, возможные последствия атаки и подробное описание любой связанной активности, известной «Лаборатории Касперского»
- Эффективная приоритизация оповещений об угрозах и (или) инцидентах с помощью подробной контекстной информации и категоризации связанных индикаторов компрометации
- Помощь в определении природы подозрительной активности (APT-угроза или атака с использованием Crimeware)
- Отправка вредоносных файлов на комплексный анализ, чтобы понять поведение и функциональность предоставленных образцов

Доступ к экспертным знаниям и ресурсам

Kaspersky Ask the Analyst предоставляет доступ к команде исследователей «Лаборатории Касперского». Мы готовы делиться знаниями и ресурсами, которые дополнят ваши возможности в области анализа угроз и реагирования на инциденты.

Threat Infrastructure Tracking

выявляет IP-адреса инфраструктур, являющихся источниками продвинутых угроз.

Threat Infrastructure Tracking

Сервис Threat Infrastructure Tracking от «Лаборатории Касперского» выявляет IP-адреса инфраструктур, являющихся источниками продвинутых угроз. Он помогает аналитикам безопасности, работающим в группах экстренного реагирования на инциденты (CERT), центрах мониторинга и реагирования (SOC) и агентствах национальной безопасности, отслеживать развертывание новых угроз и вредоносных кампаний, а затем принимать меры, необходимые для минимизации ущерба от текущих и предстоящих атак. Информация предоставляется как для определенной страны, так и для всех стран мира. Она ежедневно пополняется последними данными, полученными от Центра глобальных исследований и анализа угроз «Лаборатории Касперского».

Каждый IP-адрес сопровождается следующими вспомогательными данными:

- Название группы угроз, операций или вредоносных программ, с которыми он связан
- Информация об интернет-провайдере и автономной системе
- Набор связанных IP-адресов, на которых размещены данные
- Даты первого и последнего обращения к этому IP-адресу

Список IP-адресов можно экспортировать в машиночитаемый формат, чтобы затем их можно было загрузить в существующие решения безопасности для автоматического обнаружения угроз

Доступ к сервису

Сервис доступен на портале Kaspersky Threat Intelligence Portal через веб-интерфейс или RESTful API.

Компонент	Веб-интерфейс	API
Просмотр списка опасных IP-адресов	●	●
Фильтрация списка опасных IP-адресов по дате	●	
Фильтрация списка опасных IP-адресов по странам	●	●
Экспорт списка опасных IP-адресов	●	

Преимущества

Уровень безопасности

Понимание уровня безопасности в стране в соответствии с распространением таких инфраструктур

Выявление угроз

Выявление новых активных инфраструктур, используемых злоумышленниками в конкретной стране

Быстрое реагирование

Обеспечение быстрого реагирования на инциденты и проактивный поиск угроз в регионах

Атрибуция

Определение, кто именно из известных злоумышленников стоит за конкретными атаками

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