Аналитические отчеты
об угрозах

Kaspersky Intelligence Reporting

kaspersky активируй будущее

Kaspersky Intelligence Reporting

Отслеживание действий кибергруппировок, выявление наиболее сложных и опасных целевых атак, кампаний кибершпионажа, образцов вредоносного ПО и шифровальщиков по всему миру.

Аналитические отчеты об угрозах

Для эффективного противодействия современным киберугрозам требуется всестороннее понимание тактик, техник и процедур, используемых киберпреступниками. Несмотря на то, что командные серверы и инструменты, применяемые для проведения атак, часто меняются, злоумышленникам достаточно сложно изменить свое поведение и методы, применяемые в ходе атаки.

Понимание этих признаков позволяет заранее развернуть эффективные защитные механизмы и таким образом обезоружить киберпреступников, нарушив их планы.

Подписка на аналитические отчеты об угрозах обеспечивает постоянный эксклюзивный доступ к исследованиям «Лаборатории Касперского», предоставляя актуальные сведения о наиболее опасных угрозах.

Наши эксперты непрерывно отслеживают действия кибергруппировок, выявляя наиболее сложные и опасные целевые атаки, кампании кибершпионажа, образцы вредоносного ПО и шифровальщиков, а также новейшие тенденции в сфере киберпреступности по всему миру. Лишь небольшой процент наших расследований доступен широкой публике, в то время как постоянные клиенты «Лаборатории Касперского» всегда имеют доступ к самым актуальным сведениям о новейших угрозах. Это помогает организациям проактивно применять эффективную стратегию для своевременного обнаружения атак, а также нейтрализации и минимизации ущерба от аналогичных угроз.

200+
приватных отчетов в год

300+
профилей кибергруппировок

500+
кампаний

2500+
YARA-правил

17 000+
индикаторов компрометации

В состав аналитических отчетов входят:

Профили злоумышленников

Сопоставление с матрицей MITRE ATT&CK

Бизнес-ориентированная информация для топ-менеджмента

Глубокий технический анализ

- Методы атаки
- Использованные эксплойты
- Описание ВПО
- Описание инфраструктуры атакующих (командные центры и протоколы злоумышленников)
- Анализ эксфильтрации данных
- Атрибуция

Индикаторы компрометации (IOCs) и YARA / Sigma / Suricata-правила

Заключения и рекомендации экспертов «Лаборатории Касперского»

Преимущества

Привилегированный доступ

Не все громкие угрозы становятся известны широкой публике. Но мы предоставляем такую эксклюзивную информацию нашим клиентам еще в ходе расследования, до публичного объявления

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 / Sigma / Suricata

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

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

Ретроспективный анализ

В течение срока действия подписки доступны все ранее выпущенные закрытые отчеты

Поддержка RESTful API

Беспрепятственная интеграция и автоматизация процессов безопасности

В зависимости от специфики деятельности вашей организации предлагаем несколько типов коммерческих отчетов

Kaspersky APT Intelligence Reporting

APT Intelligence Reporting

В аналитических отчетах об APT-угрозах содержится информация о самых сложных целевых атаках, авторами которых обычно являются хорошо организованные и финансируемые кибер-группировки. В нем содержится информация о различных APT-группах по всему миру, их тактиках, техниках и процедурах (TTPs), а также о секторах экономики и регионах, на которые они направлены. В данном типе отчета основное внимание уделяется шпионской деятельности — от атак на цепочки поставок до активистских и деструктивных действий.

Эти отчеты наиболее ориентированы на крупные корпорации, государственные учреждения и организации, связанные с критической инфраструктурой, хранящие конфиденциальные данные, представляющие интерес для государственных субъектов.

Kaspersky Crimeware Intelligence Reporting

Crimeware Intelligence Reporting

Отчеты об угрозах, связанные с финансово мотивированными группировками посвящены последним тенденциям в киберпреступности, включая утечки данных, продаваемых в дарквебе, финансовое мошенничество, программы-вымогатели и вредоносное ПО, ориентированное на банкоматы и платежные терминалы. В данном отчете основное внимание уделяется кампаниям, атакам, и инструментам, основной целью которых является получение финансовой выгоды.

Этот тип отчетов особенно актуален для организаций, ведущих значительный объем бизнеса через интернет или хранящих конфиденциальные данные о клиентах, например для финансовых и платежных организаций, банков, платформ электронной коммерции.

Kaspersky ICS Intelligence Reporting

ICS Threat Intelligence Reporting

В рамках Kaspersky ICS Threat Intelligence Reporting «Лаборатория Касперского» предоставляет подробную аналитику вредоносных кампаний, нацеленных на промышленные организации, аналитику уязвимостей, обнаруженных в наиболее популярных АСУ ТП и технологиях, используемых в инфраструктурах промышленных компаний, а также предоставляет ранние предупреждения об угрозах и свежих найденных уязвимостях. Материалы создаются выделенной командой Kaspersky ICS CERT, в которой работает 20+ высококвалифицированных специалистов по исследованию угроз и уязвимостей АСУ ТП, реагированию на инциденты и анализу безопасности.

Сервис позволяет снизить время реакции на инцидент, отреагировать на инцидент оптимальным образом с меньшими потерями, снизить риски остановки работы и сократить время возможного простоя предприятия.

Другие сервисы, предоставляемые командой Kaspersky ICS CERT:

ICS Malishious Hash Data Feed

Регулярно обновляемый поток машиночитаемых данных об актуальных угрозах кибербезопасности для АСУ ТП, позволяющий упростить и автоматизировать своевременное обнаружение и расследование кибератак

ICS Vulnerability Data Feed

Регулярно обновляемый поток проверенных и уточненных данных об уязвимостях в ПО и оборудовании АСУ ТП и других решениях, широко применяемых в промышленных средах, в унифицированном машиночитаемом формате

ICS Vulnerability Data Feed в формате OVAL

Регулярно обновляемый поток OVAL-определений для автоматического обнаружения известных уязвимостей в SCADA системах и другом промышленном программном обеспечении

Kaspersky Digital Footprint Intelligence

Подробнее

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 без прямого контроля над ними. Динамические и взаимосвязанные среды дают организациям множество преимуществ. Однако постоянный рост взаимосвязей расширяет поверхность атаки, а 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, но некоторые задачи по-прежнему вызывают у них трудности, к примеру 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.

Основные возможности

Kaspersky Digital Footprint Intelligence предоставляет комплексную защиту от цифровых рисков, которая помогает компаниям отслеживать свои цифровые активы и обнаруживать угрозы в даркнет-ресурсах (deep web, darknet и dark web).

Мониторинг даркнета

Постоянный мониторинг десятков даркнет-ресурсов (форумы, блоги вымогателей, мессенджеры, тор-сайты и т. д.), выявляющий любые упоминания и угрозы, касающиеся вашей компании, клиентов и партнеров. Анализ активных целевых или планируемых атак, APT-кампаний, направленных на вашу компанию, отрасль и регионы присутствия.

Обнаружение утечек данных

Обнаружение скомпрометированных учетных данных сотрудников, партнеров и клиентов, банковских карт, номеров телефонов и другой конфиденциальной информации, которая может быть использована для проведения атаки или создания репутационных рисков для вашей компании.

Анализ сетевого периметра

Идентификация сетевых ресурсов и открытых сервисов компании, которые являются потенциальной точкой входа злоумышленников для атаки. Индивидуальный анализ существующих уязвимостей с дальнейшим подсчетом баллов и всесторонней оценкой рисков на основе системы Common Vulnerability Scoring System (CVSS), наличия общедоступных эксплойтов, опыта тестирования на проникновение и местоположения сетевого ресурса (хостинга/инфраструктуры).

Обнаружение угроз

Мониторинг вредоносной активности, которая может нанести ущерб репутации компании и/или привести к атакам на ее клиентов.

Принцип работы

Конфигурация

Инвентаризация всех цифровых активов компании

Сбор данных

Автоматизированный сбор данных из Даркнета (DarkWeb) и видимой часть сети Интернет (Surface Web), а также из базы знаний «Лаборатории Касперского»

Фильтрация

Обнаружение угроз, их анализ и приоритезация под управлением аналитиков

Оповещение

Предоставление оперативных уведомлений об угрозах на Kaspersky Threat Intelligence Portal или по API

Преимущества

Защита бренда

Выявление потенциальных угроз в режиме реального времени для защиты репутации вашего бренда, сохранения доверия клиентов, снижения риска финансовых потерь и ущерба бизнес-операциям

Вскрытие замыслов злоумышленников

Предупрежден — значит вооружен. Узнайте, что киберпреступники обсуждают в даркнете о вашей компании и планируют ли атаки

Быстрое реагирование

Дополнительный контекст для мгновенных уведомлений улучшает реагирование на инциденты и сокращает среднее время реагирования (MTTR)

Сокращение векторов атаки

Аналитические данные и рекомендации позволяют сократить количество потенциальных векторов атаки и риски информационной безопасности для организации

Оптимизация затрат

Помощь лицам, принимающим решения, в приоритезации расходов на кибербезопасность за счет выявления пробелов в текущей защите и связанных с ними рисков

Дополнительная экспертиза

Усиление ваших внутренних команд безопасности дополнительными возможностями для противостояния кибератакам и выявления угроз

Kaspersky Intelligence Reporting

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее