Kaspersky Ask the Analyst

kaspersky АКТИВИРУЙ БУДУЩЕЕ

«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.

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.

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