Kaspersky Threat Intelligence Reporting

kaspersky активируй будущее

2000+

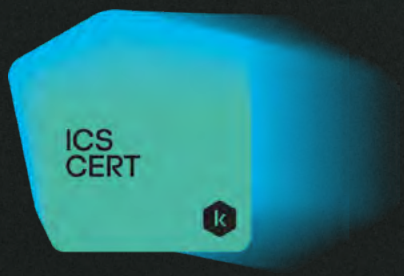
уже опубликованных отчётов

200+

новых отчётов каждый год

100 000+

часов исследований в год



Отчёты Kaspersky Threat Intelligence

Отчёты Kaspersky Threat Intelligence предоставляют организациям экспертную аналитику глобальных киберугроз, в которой технический анализ сочетается с реальным контекстом, что позволяет принимать взвешенные решения в сфере безопасности.

Структурированные сведения о злоумышленниках, включая тактики, методы и процедуры (TTP), помогают ИБ-специалистам понять, как осуществляются атаки и их потенциальные последствия.

Клиенты получают доступ к аналитическим данным из текущих расследований «Лаборатории Касперского», в том числе к результатам, которые не разглашаются публично. Это способствует более раннему выявлению угроз, проактивному обнаружению атак и снижению рисков.

Центр глобальных исследований и анализа угроз «Лаборатории Касперского» и наши эксперты расследуют сложные атаки, в том числе совершаемые APT-группировками, которые спонсируются государствами и используют уязвимости нулевого дня. Команда ICS CERT изучает угрозы для промышленных систем, анализирует потенциальные уязвимости и разрабатывает подробные инструкции по их устранению.

Аналитические данные предоставляются в форматах, ориентированных как на оперативное реагирование, так и на углубленный анализ:

Короткие отчёты

Уведомления о важных находках, включая атаки нулевого дня и компрометацию цепочки поставок

Комментарии экспертов

Сведения о ранних этапах исследований с использованием новых индикаторов компрометации (IOC)

Подробные отчёты

Комплексный анализ, включая реверс-инжиниринг и рекомендации по снижению рисков

Отчёты Kaspersky Threat Intelligence предоставляют доступ к аналитическим данным текущих расследований и позволяют выявлять новейшие угрозы. Кроме того, клиенты могут обращаться к обширному архиву отчётов об APT-угрозах, об угрозах для АСУ ТП и о ПО для финансовых преступлений.

APT-угрозы

Отчёты об APT-угрозах дают вашим специалистам постоянный доступ к расследованиям «Лаборатории Касперского», включая подробные технические сведения о выявленных кампаниях. Это помогает понять поведение APT-группировок и оценить потенциальные риски – в том числе от угроз, сведений о которых нет в публичном доступе.

Системы управления технологическими процессами (АСУ ТП)

Отчёты об угрозах для АСУ ТП помогают понять риски для промышленной среды и противостоять им. Они содержат глубокий анализ кампаний, нацеленных на производственные организации, и распространенных уязвимостей в системах и технологиях.

Crimeware

Отчёты о ПО для финансовых преступлений предоставляют своевременную информацию о вредоносных кампаниях, затрагивающих финансовые учреждения. Они содержат анализ инструментов и техник, нацеленных на банки, платежные системы и связанную с ними инфраструктуру, а также рекомендации по разработке стратегий защиты.

Целевая аудитория

Специалисты SOC

Подробные отчёты позволяют анализировать тактики, методы и процедуры злоумышленников, расширяют возможности обнаружения и приоритизации угроз с учетом контекста и степени серьезности

ИБ-инженеры

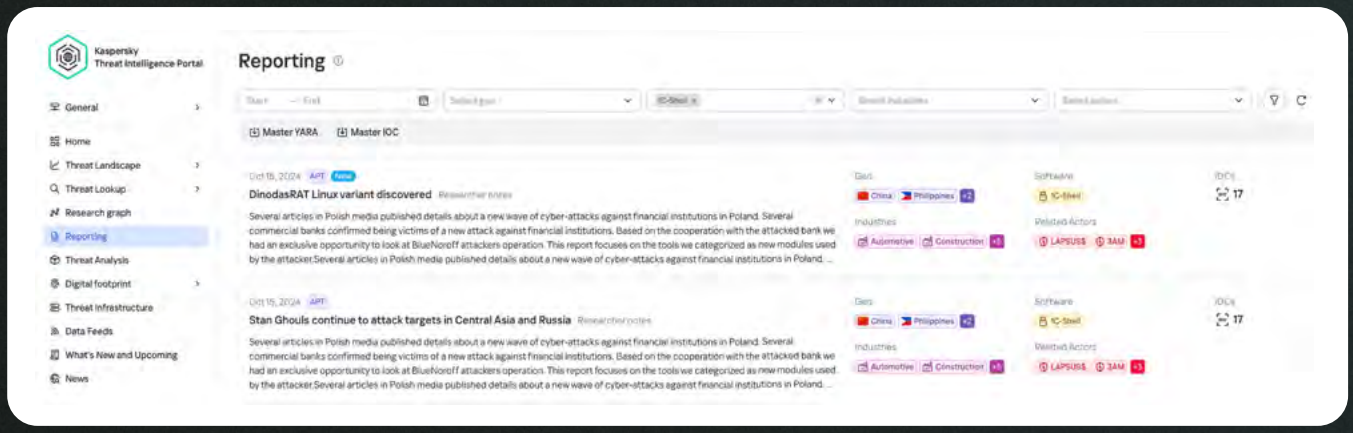
Анализ угроз помогает разрабатывать и совершенствовать алгоритмы обнаружения и сравнивать внутренние модели угроз со схемами реальных атак

Высшее руководство

Глобальная аналитика угроз – основа для принятия информированных решений о стратегии кибербезопасности и соответствующих инвестициях

Удобный и продуманный интерфейс

Доступ к отчётам Kaspersky Threat Intelligence Reporting предоставляется через понятный интерфейс с возможностями анализа.



Фильтры:

- Отрасль
- Акторы
- Категория угроз (APT/Crimeware/ICS)
- Страна
- Дата публикации
- Тип отчёта

Практическая аналитика

Каждый отчёт содержит подробные данные, которые помогают быстрее принимать обоснованные решения в условиях ограниченного времени.

Дополнительные материалы

- Процедура дешифровки
- Извлеченные файлы конфигурации

Сопоставление с данными MITRE ATT&CK

- TTP и их использование в ходе атаки

Индикаторы атаки

- Правила Suricata
- Правила YARA

Индикаторы компрометации

- Разделы реестра
- Имена служб/задач
- Мьютексы
- Домены, IP-адреса, URL-адреса
- Имена файлов и пути к ним
- Хеш-суммы файлов

Коммерческая ценность

Важнейшие данные

Аналитические данные об актуальных угрозах для вашей отрасли и региона позволяют точнее оценивать уязвимости

Актуальная аналитическая информация

Готовность к отражению APT-атак, характерных для вашего сектора, даже если они еще не затронули вашу отрасль

Глобальная видимость

Понимание распространенных во всем мире тактик, методов и процедур помогает адаптировать меры защиты к потенциальным угрозам из других регионов

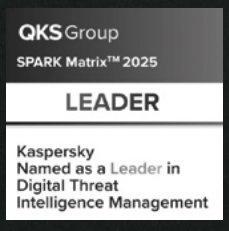
Интеграция с рабочими процессами

Интеграция аналитических данных об угрозах в существующие рабочие процессы через API позволяет внедрить и масштабировать единый протокол использования данных об обнаружениях

	Отчёты Kaspersky Threat Intelligence	SECURELIST «Лаборатории Касперского»*	Отчёты других вендоров
Источник аналитических данных	Эксклюзивная информация KSN	Эксклюзивная информация KSN	В основном из открытых источников
Индикаторы компрометации (IoC)	Все доступные	Ограниченный набор только для ознакомления	Зависят от видимости угроз
Логика обнаружения (YARA и т. п.)	Да	Нет	Нет
Тактики, методы и процедуры MITRE	Да	Нет	Нет
Доступность для акторов	Нет	Да	Да
Минимальное время между обнаружением и реакцией	Да	Нет	Нет
Включает неизвестных акторов, представляющих наибольшую угрозу	Да	Да	Ограниченные
Дополнительная информация по запросу	Да	Нет	Нет

* Официальный блог «Лаборатории Касперского», посвященный защите от вирусов, шпионских программ, хакеров, спама и других видов вредоносного ПО

Компания Frost & Sullivan признала «Лабораторию Касперского» лидером в рейтинге Frost Radar™: Cyber Threat Intelligence (отчёт за 2024 г.).



Группа QKS признала «Лабораторию Касперского» лидером в рейтинге SPARK Matrix™: Cyber Threat Intelligence за 2025 г.

www.kaspersky.ru

Консультация эксперта

#kaspersky
#truetobusiness