KSD 2022

Kaspersky Security Day

Экспертиза как основа сервисов

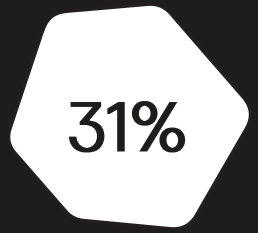
Александр Мазикин
Руководитель группы по развитию продаж сервисов

kaspersky 25 лет

Проникновение **Threat Intelligence**

Крупных организаций уже используют

Основной барьер – высокая цена коммерческих источников данных



Планируют начать использовать в течении года

Kaspersky Corporate IT Security Risks Survey 2019 - Brand13. “What is your organization's adoption of, or plans to adopt each in the next 12 months? - Threat intelligence”

Threat Intelligence Resource Hub

We are carefully watching the events unfolding in and around Ukraine. These are challenging and uncertain times but our key priority remains the same – to protect our customers in any country from cyberthreats.

- We anticipate that the current conflict will lead to a growing number of cyberthreats.
- Threat actors will be trying to exploit the ongoing crisis for their own ends.
- To confront this potential wave of cyberattacks, businesses worldwide need to have access to trusted and timely threat intelligence.

Почему Threat Intelligence это важно?

Приоритезация рисков

Позволяет сосредоточится на критических проблемах

Принятие решений за счет понимания действий злоумышленников

Повышает эффективность и скорость реагирования на угрозу

Знание тактик, техник и процедур (TTPs)

Помогает улучшить детектирование угроз

150+

Отчетов на различные темы*

* Публикуются командами исследователей

Threat Intelligence – сценарии использования

Расследования

- Инструменты для ускорения расследований
- Threat Hunting

Устранение

- Мониторинг бренда
- Takedown и блокировка ресурсов

Реагирование

- Валидация событий и обогащение
- Приотиризация уязвимостей

Детектирование

- Обнаружение инцидентов
- Отслеживание источников
- Security Enrichment

Threat Intelligence - портфолио

GREAT

Kaspersky APT Research team

Kaspersky SOC

Kaspersky Red Team

Kaspersky ICS CERT

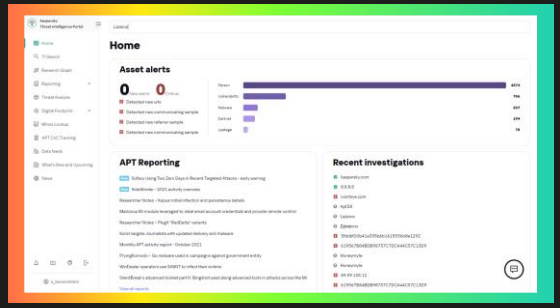
Technical — Machine-readable данные и Threat Intel Platform

Operational — Master search, research graph, sandboxing и threat attribution

Tactical — TTPs и профили злоумышленников из APT, Crimeware и ICS отчетов

Strategic — Digital Footprint Intelligence: Мониторинг, отчеты, Dark web

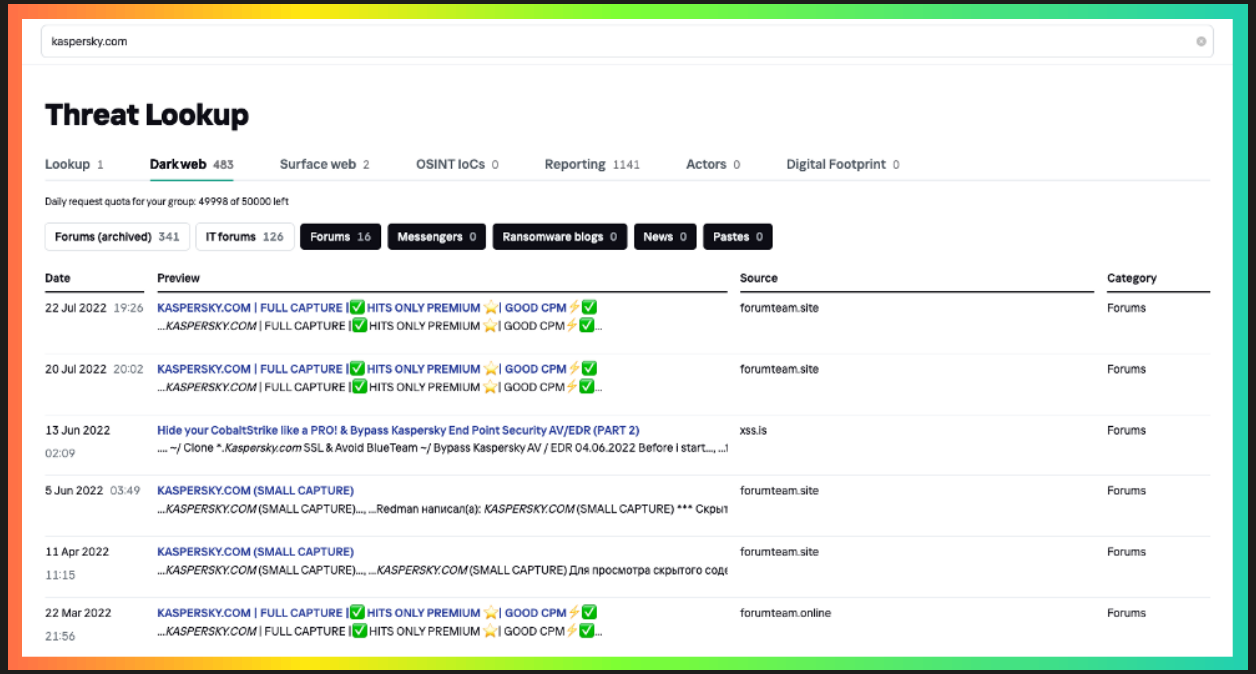
Web-Portal и API



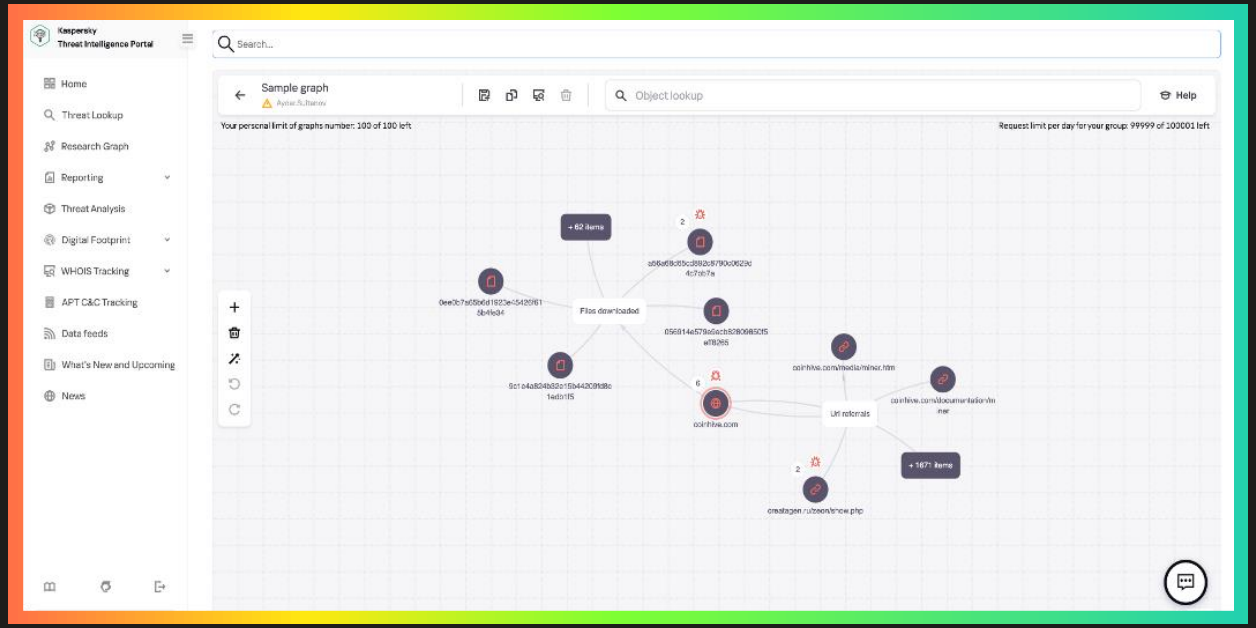
Takedown и Ask the Analyst сервисы

Портфолио Kaspersky Threat Intelligence

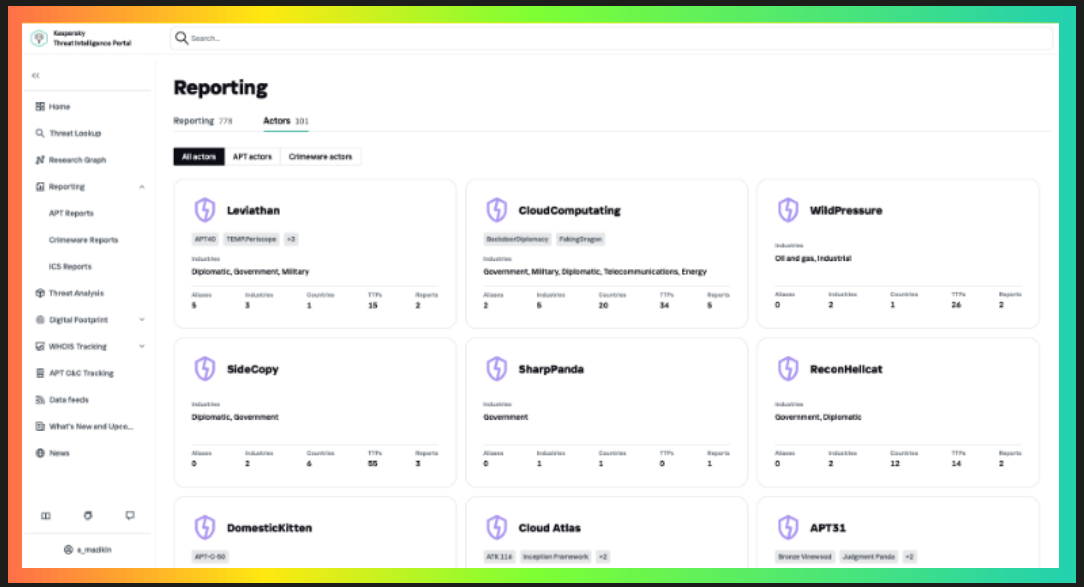
Master Search



Research Graph



Основные обновления



Основные обновления:

- Больше Actor профилей (+ Crimeware)
- ATA & Takedown релиз
- Threat Infrastructure Tracking
- OTP доступ
- Research Graph
- Threat Analysis релиз
- Master Search релиз
- Дополнительные DFI данные

DFI как защита бренда

Digital Footprint Intelligence

Стратегический сервис

- Экспертная оценка
- Периодические отчеты
- Данные от вендора
- Зловреды и угрозы
- Данные по индустриям
- Угрозы нац. уровня

- Периметр сети
- Доступные сервисы
- Service fingerprinting
- Выявление уязвимостей
- Анализ эксплойтов
- Скоринг и анализ рисков

- Surface, deep и dark web
- Активность злоумышленников
- Утечки
- Инсайдеры
- Соц. Сети сотрудников
- Утечки метаданных

- База знаний ЛК
- Анализ зловредов
- Ботнеты и фишинг
- Синкхолинг
- APT Intelligence Reporting
- Threat Data Feeds

Защита бренда

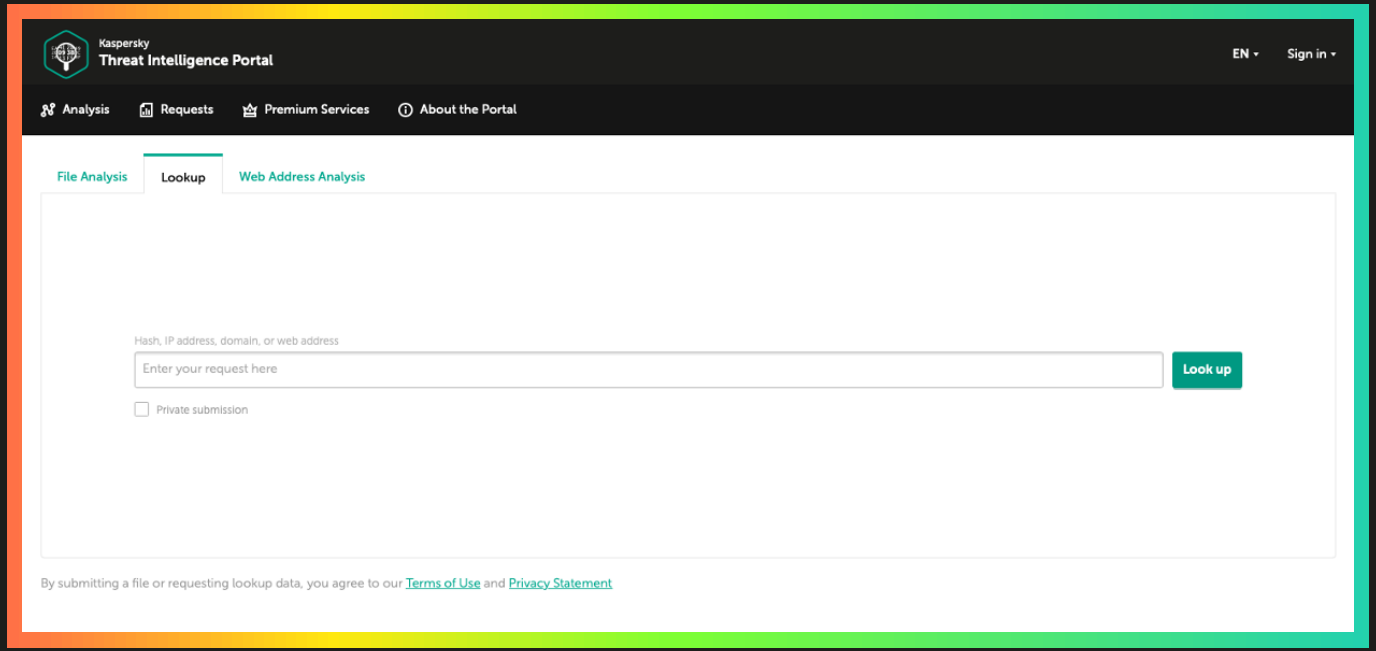
- Real-time notifications
- Сырые данные
- Ключевые слова
- Утечки
- Управление ассетами
- Takedown
- Dark web
- Соц. Сети и маркеты

Web-Portal:
real-time notifications + периодическая отчетность

Пакетное предложение

	CORE	UNIVERSAL	COMPLETE
APT Reporting	Executive summary	+	+
Crimeware Reporting	Executive summary	+	+
ICS Reporting	Executive summary	+	+
Digital Footprint Intelligence	1 отчет + мониторинг на полгода	1 отчет + мониторинг	4 отчета + мониторинг
Threat Lookup Cloud Sandbox Cloud Threat Attribution Engine	50 запросов 5 запросов 5 запросов	100 запросов 10 запросов 10 запросов	100 запросов 10 запросов 10 запросов
Threat Infrastructure Tracking	-	По стране	+
Ask the Analyst	-	5 запросов	10 запросов
Takedown Service	-	+	+

Open TIP


Kaspersky
Threat Intelligence Portal
EN
Sign in
Analysis
Requests
Premium Services
About the Portal
File Analysis
Lookup
Web Address Analysis
Hash, IP address, domain, or web address
Enter your request here
Look up
Private submission
By submitting a file or requesting lookup data, you agree to our Terms of Use and Privacy Statement

ICS Threat Intelligence

ICS Reporting

Доступ по подписке к регулярным отчетам TI с информацией об атаках, угрозах и уязвимостях, специфичных для ICS

ICS malware data feed

Feed содержит индикаторы компрометации (IOC) и метаданные для интеграции со сторонними системами SIEM

Tailored reports

Кастомизированные отчеты по анализу угроз с тактическим или стратегическим фокусом за период (квартал / год) или о локации / отрасли

ICS vulnerability data feed

Feed содержит точную и актуальную информацию для выявления уязвимостей в сетях ICS

Все исследования угроз, связанных с ICS, проводятся Kaspersky ICS CERT

- Основан в 2016 году
- Первый CERT, созданный коммерческой организацией
- Около 20 высококвалифицированных экспертов в области исследования угроз и уязвимостей ICS, реагирования на инциденты и анализа безопасности

День 1. Вводный

Что такое Threat Intelligence? Определение, классификация, цели, использование и ожидание от TI
Где, как и кем использовать?

День 2. Практика

Intelligence инструменты
Автоматизация
Hunting: инфекции, следы атак

Позиции Лаборатории Касперского

- Лаборатория Касперского топ вендор в Gartner “peerInsights”.
- GigaOm: “Лидерский набор threat intelligence решений и сервисов”.
- Forrester дал оценку “Лидер” в последнем исследовании

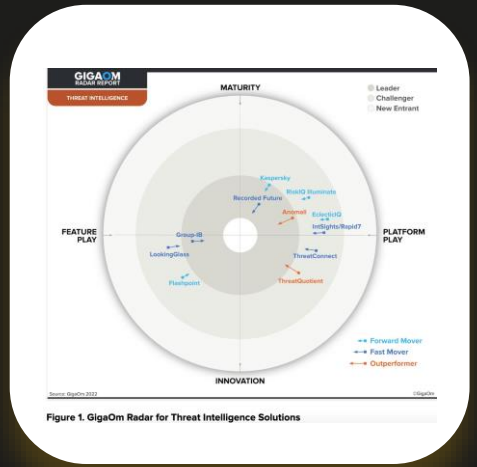


Figure 1. GigaOm Radar for Threat Intelligence Solutions

> The biggest intelligence bodies in the cyberworld are private entities – FireEye and Kaspersky have more information than any state intelligence body.

Dr. Mohamed al-Kuwaiti, Head of Cyber Security, UAE Government

Спасибо за внимание!

kaspersky 25 лет