Сервис по отслеживанию
инфраструктур
кибергруппировок

Kaspersky Threat Infrastructure Tracking

kaspersky активируй будущее

Kaspersky Threat Infrastructure Tracking

Помогает аналитикам безопасности отслеживать развертывание новых угроз и вредоносных кампаний, а затем принимать меры, необходимые для минимизации ущерба от текущих и предстоящих атак.

Kaspersky Threat Infrastructure Tracking

Сервис по отслеживанию инфраструктур кибергруппировок

Сервис Threat Infrastructure Tracking 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

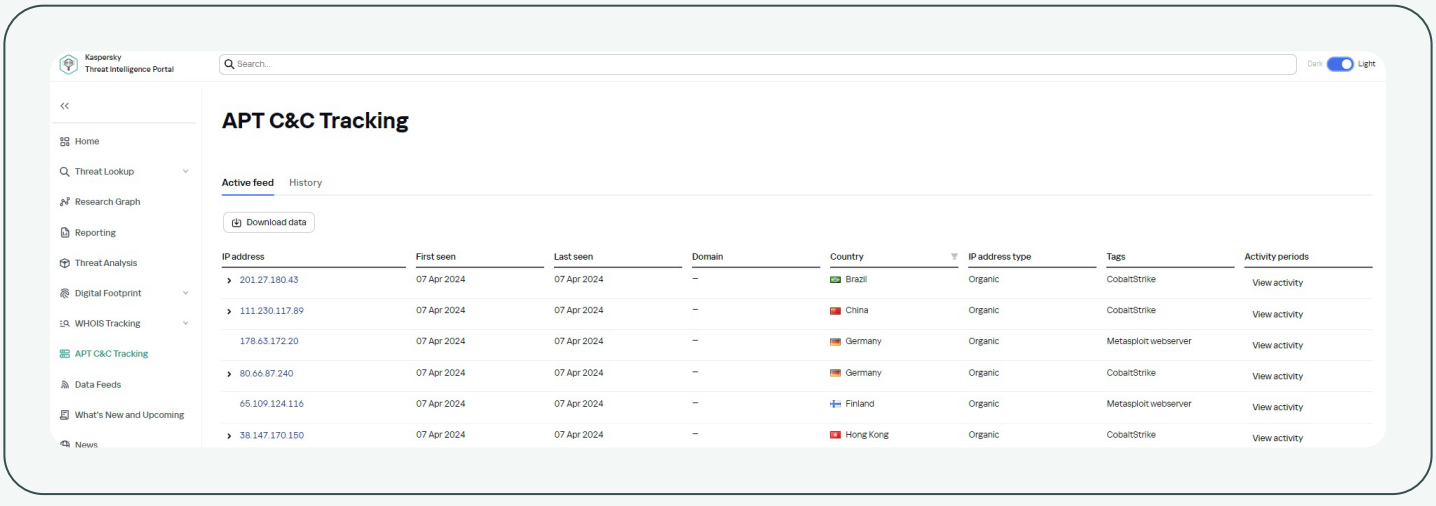
Набор связанных IP-адресов, на которых размещены данные

Информация об интернет-провайдере и автономной системе

Даты первого и последнего обращения к этому IP-адресу

Возможность экспорта

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

Атрибуция

Определение, кто именно из известных злоумышленников стоит за конкретными атаками

Быстрое реагирование

Обеспечение быстрого реагирования на инциденты и проактивный поиск угроз в регионах

Kaspersky Threat Infrastructure Tracking

Подробнее

www.kaspersky.ru

#kaspersky
#активируйбудущее