



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 продвинутой угрозы. 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.

The screenshot shows the Kaspersky Threat Intelligence Portal interface. The main content area displays a table titled "APT C&C Tracking" with an "Active feed" tab selected. A "Download data" button is visible above the table. The table has columns for IP address, First seen, Last seen, Domain, Country, IP address type, Tags, and Activity periods. The data rows are as follows:

IP address	First seen	Last seen	Domain	Country	IP address type	Tags	Activity periods
201.27.180.43	07 Apr 2024	07 Apr 2024	-	Brazil	Organic	CobaltStrike	View activity
111.230.117.89	07 Apr 2024	07 Apr 2024	-	China	Organic	CobaltStrike	View activity
178.63.172.20	07 Apr 2024	07 Apr 2024	-	Germany	Organic	Metasploit webserver	View activity
80.66.87.240	07 Apr 2024	07 Apr 2024	-	Germany	Organic	CobaltStrike	View activity
65.109.124.116	07 Apr 2024	07 Apr 2024	-	Finland	Organic	Metasploit webserver	View activity
38.147.170.150	07 Apr 2024	07 Apr 2024	-	Hong Kong	Organic	CobaltStrike	View activity

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

© 2024 АО «Лаборатория Касперского». Зарегистрированные товарные знаки и знаки обслуживания являются собственностью их правообладателей.

[#kaspersky](#)
[#активируйбудущее](#)