Kaspersky Threat Infrastructure Tracking

Introduction

Kaspersky Threat Infrastructure Tracking reveals the IP addresses of infrastructures connected to advanced threats. This helps security analysts working in CERTs, national SOCs, and national security agencies to monitor the deployment of new malware, so that they can take the necessary measures to mitigate ongoing and upcoming attacks. The information is provided for a specific country, or worldwide. It is updated daily with the most recent findings of Kaspersky's Global Research and Analysis Team, which has a proven track record of discovering crimeware and APT campaigns across the world. Each IP address is provided with additional supporting context such as:

The name of the threat group, operation or malware it is associated with

Internet service provider and an autonomous system

Collection of associated IP addresses hosting information

Dates when this was first and last seen

The list of IP addresses can be exported to a machine-readable format, so you can upload it to existing security solutions to automate threat detection.

The service is available on the Kaspersky Threat Intelligence Portal via its web interface or RESTful API:

Feature	Web interface	API
View a list of dangerous IP addresses	●	●
Filter a list of dangerous IP addresses by date	●	
Filter a list of dangerous IP addresses by country	●	●
Export a list of dangerous IP addresses	●	

Benefits:

●

Understand a country's security posture related to the pervasiveness of such infrastructures

●

Identify active threat infrastructures in a particular country

●

Enable accelerated incident response and threat hunting activities in regions

●

Attribute attacks to known threat actors

Kaspersky Threat Infrastructure Tracking

Learn more

www.kaspersky.com