kaspersky BRING ON THE FUTURE

Kaspersky Threat Attribution Engine

Tracking, analyzing, interpreting and mitigating constantly evolving IT security threats is a massive undertaking. Setting aside all the hype, threat intelligence is of true value, and threat attribution is a critical element here.

Product highlights:

- Provides instant access to a repository of curated data about thousands of APT actors, samples and broader threats (via the anti-virus engine)
- Allows efficient automated or manual threat prioritization and alert triage
- Functionality to add private actors and samples, educating the product to detect samples that are similar to files in your private collection
- Manual sample upload and an enhanced REST API for integration with automated workflows
- Can be deployed in a secure, air-gapped environment, to protect your systems and data as well as meeting any compliance requirements
- Supports deployment on Amazon Web Services (AWS) enabling quick product setup and saving costs as no need to invest in hardware upfront
- Export to YARA rules for further automated search/scanning for similar files or integration with third-party solutions
- Export to STIX 2.1 format (TXT and JSON formats are also supported) for further automated analysis of security logs or integration with third-party solutions/ security controls
- Functionality for unpacking password-protected archives with custom passwords
- Access to documentation and End User License Agreement (EULA) in the web interface
- Ability to attribute in parallel files that are sent for analysis in one request

There's a good reason why threat attribution plays such a significant role in cybersecurity. The average time lag between detecting and responding to highly sophisticated threats can be frustratingly protracted, due to the complex investigation and reverse engineering processes involved. In many cases, this delay can give attackers enough time to reach their goals. Correct and timely attribution helps not only to shorten incident response times from hours to minutes, but also to reduce the number of false positives.

Identifying a targeted attack, profiling the attackers and creating attribution factors for the different threat actors is a long and complex job, which can take years. Creating a working attribution also requires a large amount of data accumulated over time, as well as a highly-skilled team of researchers with the relevant investigation experience. These researchers will commonly follow the activity of different groups, and populate a database with all the pieces of information accrued. This database then becomes a valuable resource that can be shared as a tool.

Kaspersky Threat Attribution Engine incorporates a database comprising APT malware samples and clean files gathered by Kaspersky experts over the last 25 years and more. We track 1100+ threat actors and campaigns and release 120+ threat intelligence reports a year. Our ongoing research supports an APT collection which contains some 83,000 files. This improves false flag detection and, in conjunction with the use of automated tools, results in outstandingly accurate levels of attribution.

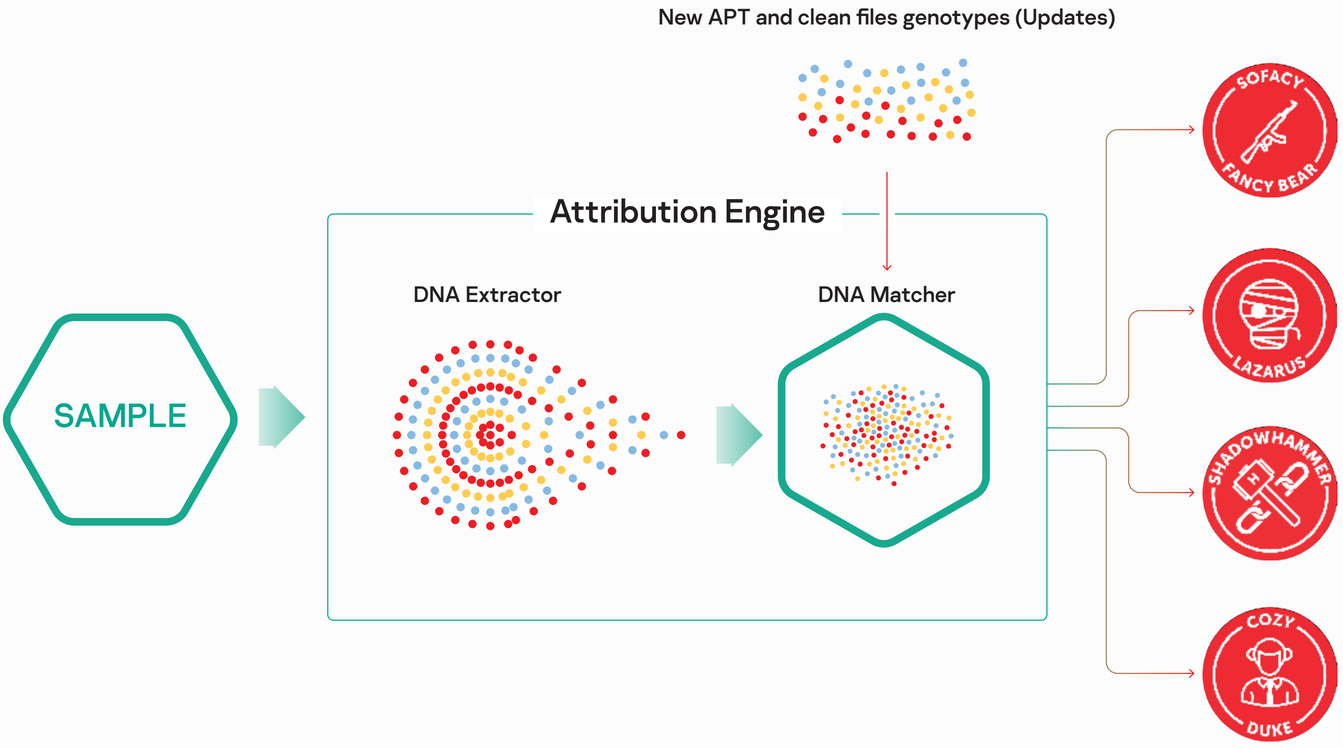
The product offers a unique approach to comparing similar samples while ensuring near-zero false positive rates. Any new attack can quickly be linked to known APT malware, previous targeted attacks and hacker groups, helping you to distinguish high-risk threats from less serious incidents, so you can take timely protective measures to prevent an attacker from gaining a foothold in your system.

How it works

To link malware to attribution entities, Kaspersky Threat Attribution Engine uses a unique proprietary method of searching for similarities between files. This method involves:

1. Analyzing the genetics of a sample by extracting the following elements from its code:
   a) Genotypes — distinctive pieces of binary code.
   b) Strings — distinctive strings of characters.
2. Automatically searching the analyzed files for genotypes and strings which are similar to genotypes and strings of APT samples previously analyzed, or already linked to attribution entities.
3. Based on similar genotypes and strings found in APT samples, providing a report on the origin of the analyzed sample, related attribution entities, and any similarities between this sample and known APT samples.

The product can be deployed in secure, air-gapped environments, restricting any 3rd party from accessing the processed information and submitted objects. An API connects the Engine to other tools and frameworks in order to implement attribution into existing infrastructure and automated processes.



Kaspersky Threat Attribution Engine

Additional benefits:

- Kaspersky Threat Attribution Engine calculates the reputation score of the sample and reveals its genetics and code attribution. This provides insights into the origin of the sample and can enable its attribution to possible authors.
- Your security team can add your own private attribution entities and related samples to the Kaspersky Threat Attribution Engine database. The team can then educate the application to attribute submitted samples to these private attribution entities and samples.
- With Kaspersky Threat Attribution Engine, the attribution process takes only seconds, compared to the months and years required in the past.

Kaspersky Threat Attribution Engine further extends and strengthens the Kaspersky portfolio for national cybersecurity agencies and commercial Security Operations Centers (SOCs) by supporting them in establishing an effective incident management process.

Kaspersky Threat Attribution Engine significantly improves security operations, helping to:

- Rapidly attribute files to known APT actors, revealing the motivations, methods and tools behind cyber incidents;
- Quickly evaluate whether you are the target of an attack or a side victim, so you can initiate the proper containment and response procedures;
- Ensure effective and timely APT threat mitigation based on actionable threat intelligence provided in Kaspersky APT Intelligence Reporting.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tomorrow.

Know more at kaspersky.com/transparency

Proven.
Transparent.
Independent.