kaspersky BRING ON THE FUTURE

Kaspersky Threat Attribution Engine

Tracking, analyzing, interpreting and mitigating constantly evolving IT security threats is a massive undertaking. Threat intelligence has true value beyond the current hype of an emerging pocket in the information security industry and threat attribution is probably the most prominent point of interest and contention when it comes to threat intelligence.

Product highlights:

- Provides instant access to a repository of curated data about hundreds of APT actors and samples
- 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 you don't need to invest in hardware upfront
- Export to YARA rules fur 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

And it has a clear reason for that. An average time from detection to response of highly sophisticated threats is usually too long due to complex investigation and reverse engineering processes. In many cases it is enough for the attackers to reach their goals. Correct and timely attribution helps not only to shorten incident response times from hours to minutes but also reduce the number of false positives.

Identifying a targeted attack, profiling the attackers and creating attribution factors for the different threat actors is long and thorough job; it can take years. The creating working attribution also requires the big amount of accumulated data since years as well as highly-skilled team of researchers with the investigation experience. In common, researchers follow the activity of different groups and populate the database with the bits of information. And the database become a valuable resource that can be shared as a tool.

Kaspersky Threat Attribution Engine incorporates the database of APT malware samples and clean files gathered by Kaspersky experts for the last 22 years. We track 600+ threat actors and campaigns with 120+ APT Intelligence reports released every year. Our ongoing research supports the actuality of the large APT collection which contains 60K+ files. It improves the false flags detection and make the attribution as much accurate as possible using the automated tools.

The product enables the unique approach for comparing samples for their similarity while ensuring zero false positive rates. It can quickly link a new attack to known APT malware, previous targeted attacks and hacker groups, helping to see the high-risk threat among less serious incidents and take timely protective measures to prevent an attacker from gaining a foothold in the system.

How it works

Kaspersky Threat Attribution Engine analyzes the "genetics" of malware looking for code similarity with previously investigated APT samples and linked actors in an automated way. It compares the "genotypes", i.e. small binary pieces of the decomposed files, with the APT malware samples database and provides a report on malware origin, threat actors and file similarity with known APT samples. Moreover, the product allows security teams to add private actors and objects to its database and educate the product to detect samples that are similar to files in your private collection. With the Threat Attribution Engine the attribution process only takes seconds comparing to the years it was required in the past.

The product can be deployed in a secure, air-gapped environment restricting any 3rd party from accessing the processed information and submitted objects. There is an API interface to connect the Engine to other tools and frameworks in order to implement attribution into existing infrastructure and automated processes.