REVERSINGLABS

ReversingLabs Spectra Sandbox APIs

Dynamic Analysis or “sandboxes” have been a fundamental security tool for performing deep analysis of evasive and unknown threats in isolated environments.

ReversingLabs Spectra Intelligence introduces a new set of APIs that support the ability to retrieve file behavior reports, or to submit files for detonation in the ReversingLabs Spectra Sandbox.

For organizations looking to remove the high cost of deploying, configuring and maintaining a local sandbox, require a highly available and scalable solution, and are open to submitting local files to the cloud, these new Spectra Intelligence APIs or equivalent services in the ReversingLabs Spectra Analyze, a malware analysis and threat hunting workbench, will provide dynamic analysis results from the cloud.

TCA-0106 Dynamic Analysis Report

The Dynamic Analysis Report service allows users to retrieve dynamic analysis reports for files or URLs executed in the ReversingLabs Spectra Sandbox.

Privacy

Whether submitted files, dropped files, PCAP files, screenshots or memory strings dumps will be available for download to other ReversingLabs customers or not, depends on the role configured for the Spectra Intelligence account used to upload files that are submitted for detonation in a sandbox.

If the account is configured to upload all files as shareable (not private), then other ReversingLabs customers will be able to access their analysis results (metadata), and will be able to download dropped files, PCAP files, screenshots, or memory strings dump files generated upon file execution.

If the account is configured to upload all files as not shareable (private), then other ReversingLabs customers will only be able to access analysis results for the files, but will not be able to retrieve dropped files, PCAP files, or memory strings dump files. These will only be available to the user account that uploaded the file.

Dynamic Analysis Report

- **General info:**
  - sample hashes: MD5, SHA1, and SHA256
  - classification (from a sandbox)
  - risk score (the trustworthiness or malicious severity of a sample)
  - threat names (a list of unique threat names within the analyzed sample)
  - analysis timestamp
  - analysis duration
  - platform on which the sample was detonated (Win7/Win10/Win11/macOS11/Linux)
    - configuration details for selected platform (e.g. Win10 x64, Office 2016, Java 8 Update 191, Acrobat Reader DC 19, Flash ActiveX 29, and Internet Explorer 11)

- **Analysis history (merged report only):** overview of all dynamic analyses performed on the file (analysis_id, platform, configuration, detonation time, sample classification...)
- **MITRE ATT&CK:** list of tactics and techniques identified by the sandbox
- **Signatures:** Abstracted behaviors, attributes, and content identified during analysis
- **Network analysis**
  - Network communication (HTTP requests, DNS requests, contacted domains - DNS resolutions, TCP/UDP communication)
- **Behavioral analysis:**
  - **Process tree:** processes generated while executing the sample in the sandbox to get the process tree for a file
    - **mutexes** (mutex created, mutex opened)
    - **file system actions** (files read, opened, copied, deleted, downloaded...)
    - **registry actions** (registry keys opened, set, deleted)
    - **process actions** (processes created, injected, terminated, requested)
    - **service actions** (services started, stopped, paused, resumed, restarted)
    - **modules loaded**
- **Malware configurations:** configurations captured while executing the file.
- **Network alerts:** list of alerts from Snort (https://www.snort.org/faq/what-is-snort)
- **Sigma detections:** Sysmon events, Windows event logs, and operating system process creation events captured during the detonation of malware in the sandbox. Sigma rules are an open source signature format that can be used to describe these log events in a generic manner. They can be converted and applied to many log management or SIEM systems.
- **Dropped/created files:** list of hashes (SHA256/SHA1/MD5) of files that were dropped while executing the sample. Sandbox classification and metadata will be provided for each file. Report also provides a link to download all files dropped during the file execution.
- **PCAP file:** Contains a link to download the PCAP file with all the network traffic generated during sample execution.
- **Memory strings:** Contains a link to download strings from a memory dump captured during file execution.
- **Screenshots:** Contains a link to download screenshots captured during file execution.

TCA-0207 Dynamic Analysis

The Dynamic Analysis service allows users to submit a file or URL for detonation in ReversingLabs Spectra Sandbox.

There are a couple of different profiles for file detonation:

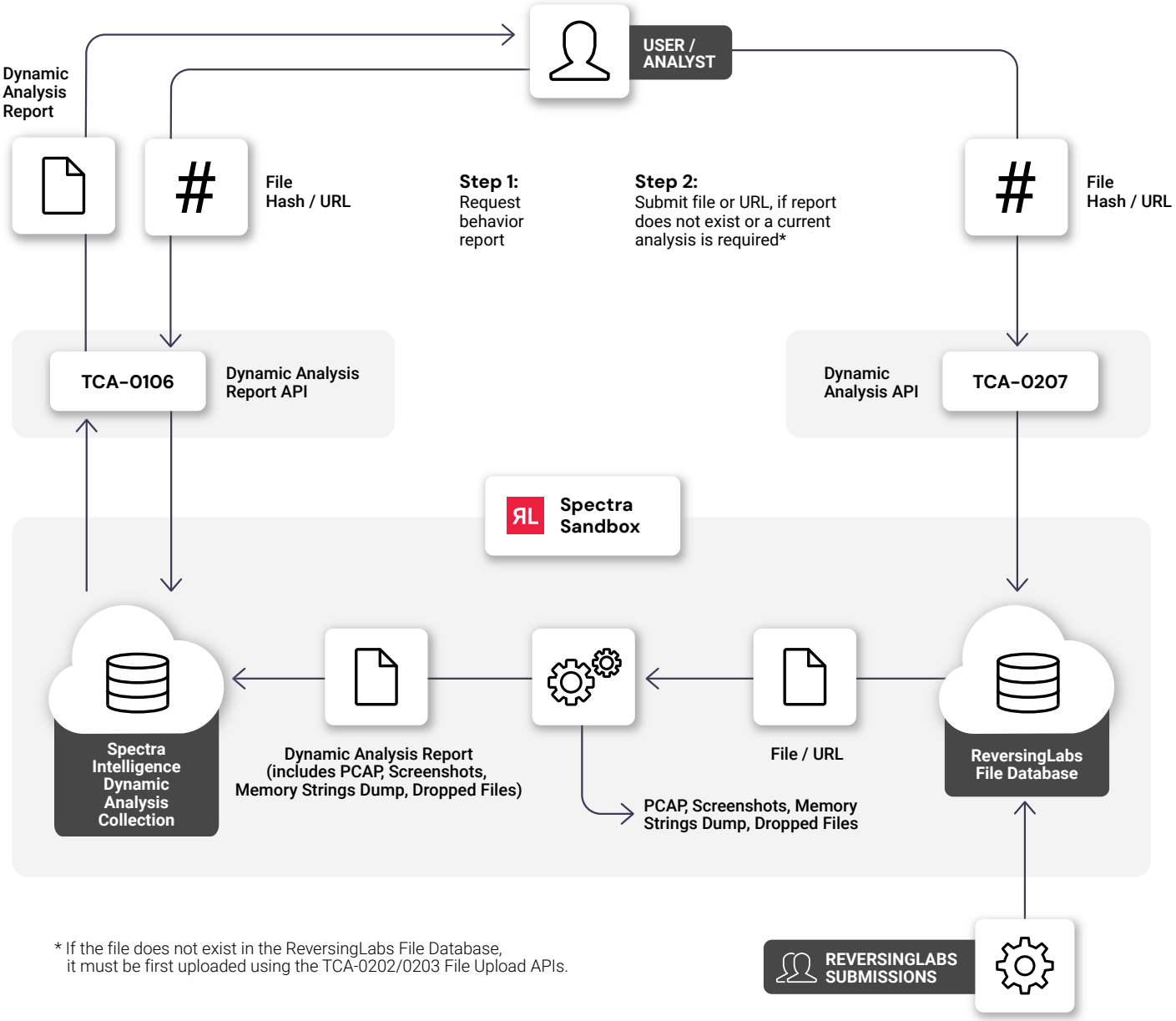
- Win11 22H2
- Win10 x64
- Win7 x64
- macOS 11
- Linux

The report on the performed analysis can be retrieved via the **TCA-0106 Dynamic Analysis Report** service.

Other key notes:

- Files up to 400MB in size supported
- Supported detonating samples in a simulated network environment
- Sample can be simultaneously submitted for analysis to multiple sandbox environments
- The analysis report within 10min from submission

ReversingLabs Spectra Sandbox APIs are available as part of the RLAPI bundle or a la carte SKUs.



* If the file does not exist in the ReversingLabs File Database, it must be first uploaded using the TCA-0202/0203 File Upload APIs.

Get started!

Improve your detection efficacy with a powerful threat intelligence solution with up-to-date threat classification

REQUEST A DEMO

reversinglabs.com

REVERSINGLABS

Worldwide Sales +1.617.250.7518
sales@reversinglabs.com