ReversingLabs Dynamic Analysis APIs

Introduction:

Dynamic Analysis or "sandboxes" have been a fundamental security tool for performing deep analysis of evasive and unknown threats in isolated environments.
ReversingLabs TitaniumCloud Sandbox introduces a new set of APIs that support the ability to retrieve file threat intelligence based on existing dynamic analysis reports, or to submit samples to the ReversingLabs cloud for analysis.

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 TitaniumCloud APIs or equivalent services in the ReversingLabs A1000 Malware Analysis Workbench will provide dynamic analysis results from the cloud.

NEW TCA-0106 File Dynamic Analysis Report

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

This service returns two types of reports: merged reports and specific reports.

- If the user provides only the file SHA1 hash to retrieve a report, the response will contain a merged report with an overview of all dynamic analyses performed on the file. Most objects in the merged report include lists of analysis IDs, allowing the users to retrieve specific reports for more information about items of interest.
- If the request includes the /latest query parameter, or an analysis_id matching an existing report, the report will contain information specific to that execution.
  The latest available report for sample per platform (win7/win10) will contain download links for the network traffic PCAP file and memory strings dump file captured during that latest analysis.

Files can be submitted for dynamic analysis using the TCA-0207 File Dynamic Analysis service.

Privacy

Whether submitted files, dropped files, PCAP files or memory strings dumps will be available for download to other ReversingLabs customers or not, depends on the role configured for the TitaniumCloud 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, 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)
  - analysis timestamp
  - analysis duration
  - platform on which the sample was detonated (Win7 or Win10)
    - 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
- **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. ReversingLabs uses an internal algorithm to filter and store dropped files in order to provide customers with the most interesting and valuable files. That said, not all files dropped during the file execution will be available for download.
- **PCAP file:** Contains a link to download the PCAP file with all the network traffic generated during sample execution. Retention period is 14 days.
- **Memory strings:** Contains a link to download strings from a memory dump captured during file execution. Retention period is 14 days.
- **Screenshots:** Contains a link to download screenshots captured during file execution. Retention period is 14 days.

  Expected daily contribution of new Dynamic Analysis reports: 50K - 100K

  Part of the RLAPI Bundle: YES.

NEW TCA-0207 File Dynamic Analysis

The File Dynamic Analysis service allows users to submit a file for detonation in ReversingLabs TitaniumCloud Sandbox. A user submits a file to be executed in the sandbox by sending the request with the file SHA1 hash and profile. There are two different profiles for file detonation:

- Win10 x64 (MS Office 2007, Java 8, update 261, Adobe Reader 2020.012.20048, Firefox 62.0.3, Google Chrome 69.0.3497.100, Microsoft Edge 42.17134.1.0, Internet Explorer 11) *
- Win7 x64 (build 760, MS Office 2007, Java 7, update 45, Adobe reader 8.1.2, Firefox 37, Google Chrome 51.0.2704.84, Internet Explorer 8) *

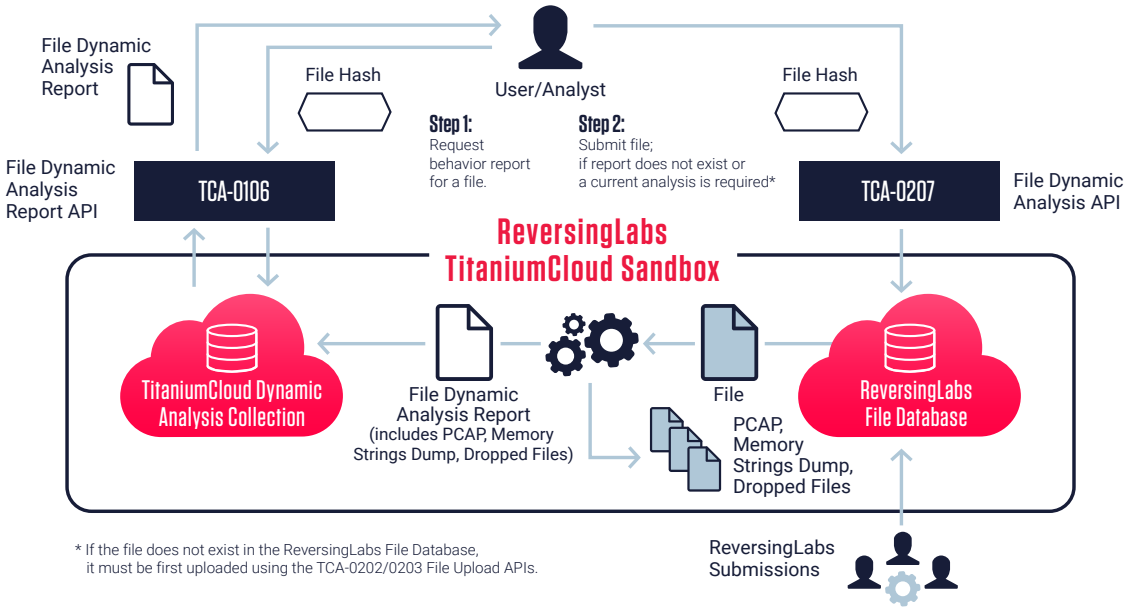
The API response will provide an analysis_id that can be used to obtain the report for that dynamic analysis run. The report on the performed analysis and file behavior can be retrieved via the **TCA-0106 File Dynamic Analysis Report** service.

Other key notes:

- To submit a file for analysis, it should exist in the ReversingLabs environment. If it does not exist, it must first be uploaded using the TCA-0202/0203 File Upload API.
- Samples must not exceed the maximum size limit of 100 MB.
- Samples can be detonated in a simulated network environment. If this option is selected, samples will be executed without connecting to the Internet (attacker) to get further instructions and will use a simulated network instead.
- Supported file types:
  - Windows executables: exe, dll, bat, chm, wsf, js, jse, vbs, vbe, ps1, cmd, pif, lnk, scr, cpl, hwp
  - Microsoft Office: DOC(X)(M), XLS(X)(M), PPT(X)(M), msg, eml
  - PDF documents
  - ZIP files
  - Java: jar
  - Misc: crx (chrome extension)
- Samples can be simultaneously submitted for analysis to multiple sandbox environments (Win7/Win10). Each analysis will get a unique analysis_id.
- If the user submits a hash for a file that is already being analyzed in the sandbox environment specified in the request, the service will respond with the analysis_id of the task in progress.
- The dynamic analysis report is expected to be ready within 10min from file submission

Part of the RLAPI Bundle: YES. Available with limited 5 submissions per day, with the option to purchase additional tiers of service via RLAPI Enhancement or à la carte SKUs.

* Current configuration. Supported environments will potentially change with subsequent updates.



REVERSINGLABS
Worldwide Sales : +1.617.250.7518
sales@reversinglabs.com