REVERSINGLABS

ReversingLabs Network Intelligence APIs

Detecting Modern Threats beyond the Payload

Introduction:

File-based threats continue to evolve as destructive objects. These "payloads" provide the software which potentially compromises your employees, your enterprise infrastructure & data, and potentially your e-business services. Exposing intelligence about those network-centric threats provides the additional visibility needed to respond and adapt your defenses.

ReversingLabs provides several APIs, and has introduced two new API services that bring network threat intelligence into its mix of authoritative file and digital certificate intelligence:

- TCA-0401 URI to Hash Search
- TCA-0402 URI Statistics
- TCA-0403 URL Threat Intelligence
- TCA-0404 Analyze URL

NEW TCA-0403 URL Threat Intelligence

This service returns threat intelligence data for the submitted URL. The report contains the ReversingLabs URL classification, URL reputation from various reputation sources, metadata for performed URL analyses, and the maliciousness of files downloaded from the submitted URL. The service also provides the option to get a list of these downloaded files along with classification and other file metadata. TCA-0403 provides a user with:

URL Classification

- URL classification based on the proprietary ReversingLabs algorithm that takes into account 3rd party URL reputation and reputation of the files downloaded during a URL analysis

3rd party URL Reputation

- ReversingLabs continually consults numerous malicious URL sources to get URL reputation, such as - Netstar, PhishTank, AlienVault, Comodo Valkyrie Verdict, MalSilo, Malware Domain Blocklist, OpenPhish, URLhaus, VX Vault, Phishstats, ADMINUSLabs

Information about performed analyses and statistics of files downloaded from a URL When a URL is analyzed one or more times, the report will provide the following data:

- First/last URL analysis time
- For every analysis – Analysis_id, final URL (if the original URL redirects), URL availability status (online/offline), HTTP response code, serving IP address, URL hosting domain
- Statistics of malicious | suspicious | known | unknown files downloaded from the submitted URL (across all analyses)
- The most common threats downloaded from the URL
- History of previously performed analyses

The list of files downloaded from a URL

- A list of file hashes downloaded from a URL – All time / last analysis / specific analysis
- Hashes returned by this endpoint can be filtered by classification - malicious / suspicious / known / unknown, e.g. the user can request a list of files classified only as malicious that were downloaded from a URL
- The user can get rich metadata for every downloaded file without having to call additional file reputation & metadata APIs (TCA-0101 File Reputation or TCA-0104 File Analysis - Hash). Additionally, this TitaniumCloud product comes with the URL Analysis Notification Feed (TCF-0301), serving a continuous list of previously submitted URLs that were analyzed to completion and their reports are ready. Using this feed, users can get information when the analysis over the submitted URL is finished and the report ready, or use the feed as an additional interesting URL source.

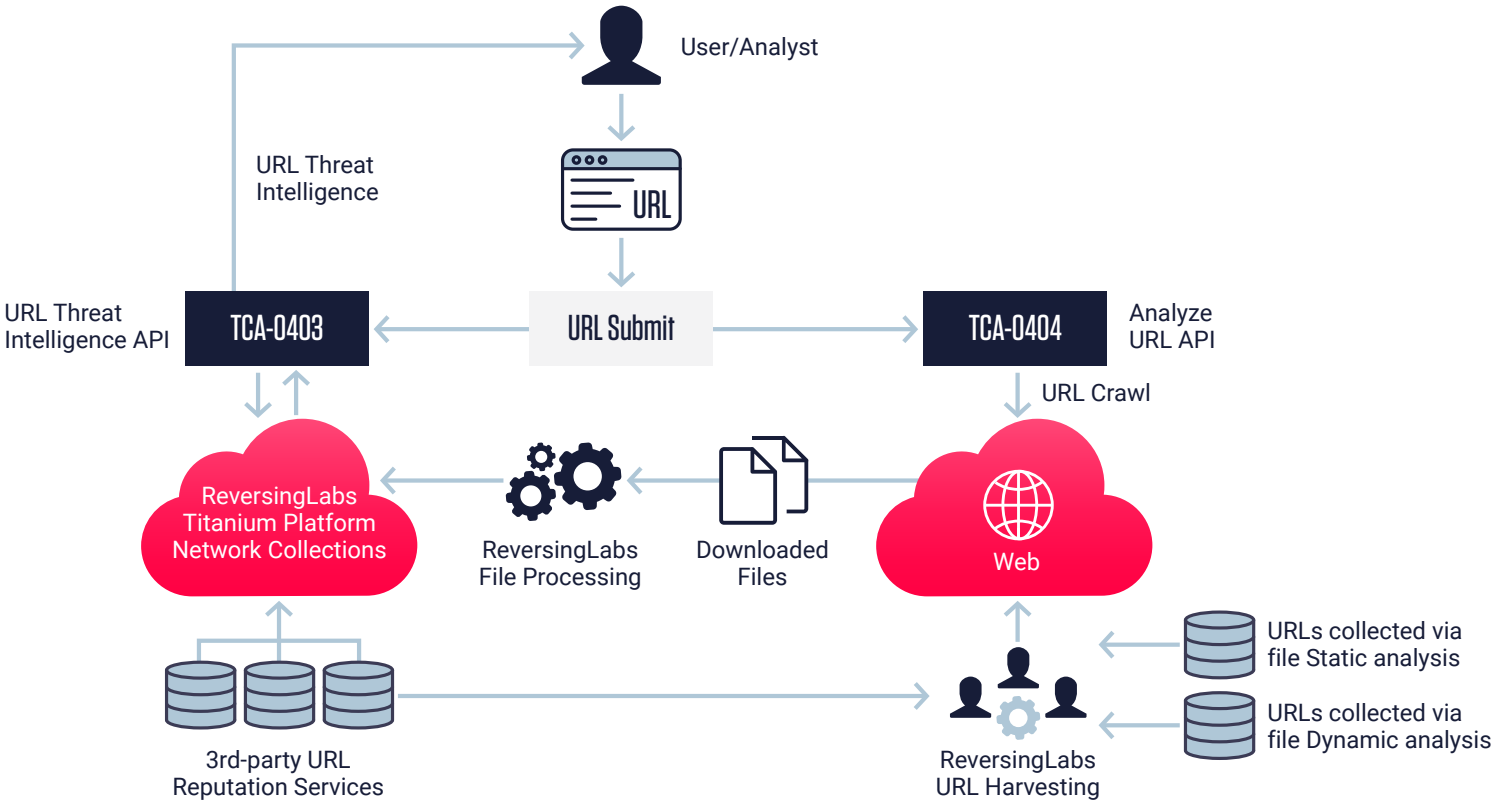
Part of the RLAPI Bundle: YES.

NEW TCA-0404 Analyze URL

This service allows users to submit a URL for analysis. Basically, the analysis is a crawling process that will start looking for files to download from the submitted URL. When downloaded, the files are automatically sent for analysis to the ReversingLabs file processing pipeline. TCA-0404 provides:

- Support for HTTP/HTTPS protocols
- URL analysis service supports redirects, i.e. a crawl will be performed on the final URL
- Files are downloaded only from the submitted URL, no recursion (crawl depth = 1)
    - E.g. if a user submitted the following URL: http://www.example.com/freshcontent, only that URL will be crawled and http://www.example.com/freshcontent/newest will not
- Implements automatic re-crawls in a regular cadence
    - To retrieve new malware versions/mutations deployed on the same URL
    - To retrieve new malware files deployed on website/opendirectory
- Maximum of 50 samples per crawl
- Maximum size of each downloaded sample – 100 MB
- URL analysis and report generation are expected to complete within 10 min
- Information about when the analysis on a submitted URL is done, downloaded files processed and report ready can be retrieved using the URL Analysis Notification Feed (part of TCA-0403 URL Threat Intelligence). The report will provide information about the performed analysis and reputation of files downloaded from the URL. The report, along with a list of samples downloaded from the submitted URL, can be retrieved via the TCA-0403 URL Threat Intelligence.

Part of the RLAPI Bundle: NO. Offered as 'a la carte'.



REVERSINGLABS

Worldwide Sales : +1.617.250.7518
sales@reversinglabs.com