REVERSINGLABS

ReversingLabs Network Threat Intelligence APIs

Network threat intelligence is a key component of a comprehensive cybersecurity strategy, providing the knowledge and insights needed to protect against evolving cyber threats and reduce the impact of security incidents. It helps organizations understand the evolving threat landscape.

This understanding is essential for anticipating and preparing for new types of attacks, as well as for adjusting security strategies to address current and emerging threats. With timely and accurate threat intelligence, organizations can respond more effectively to security incidents.

ReversingLabs Network APIs

TCA-0407 Network Reputation

This service provides a fast and lightweight reputation verdict for the submitted URL, domain, or IP address. The REST API response provides:

- **ReversingLabs classification** (only for URLs)
- Overview of detections from our network threat intelligence partners
- **The category of the URL** (eg. phishing)
- Indicator if malware samples are found to be associated with the given network location. The service allows single and bulk queries (up to 100 records per query)

TCA-0408 Network Reputation Override

This service enables overrides of URL reputation. Overrides are visible only to users within the same organization. The service allows single and bulk queries (up to 100 records per query).

TCA-0403 URL Threat Intelligence

This service returns a full threat intelligence report for the submitted URL. It provides a user with the report containing:

- **URL Classification** (based on the proprietary ReversingLabs algorithm)
- **Third-party URL reputation and categorization** - ReversingLabs continually consults 20+ quality sources to get URL reputation
- **Information about performed crawls** containing:
  - Statistics of files downloaded from a URL (mapped to classification)
  - Final URL (if the original URL redirects)
  - URL availability status (online/offline)
  - Returned HTTP response code
  - Serving IP address
  - URL hosting domain
- **The most common threats** (malware family, type) **downloaded** from the submitted URL
- History of previously performed analyses

©2024 ReversingsLabs All Right Reserved

Additionally, through separated endpoints, the service provides:

- **Files downloaded from a URL** (with rich metadata and classification)
- **URL Analysis Notification Feed** - a continuous list of previously submitted URLs that are analyzed to completion, and their reports are ready

TCA-0404 Analyze URL

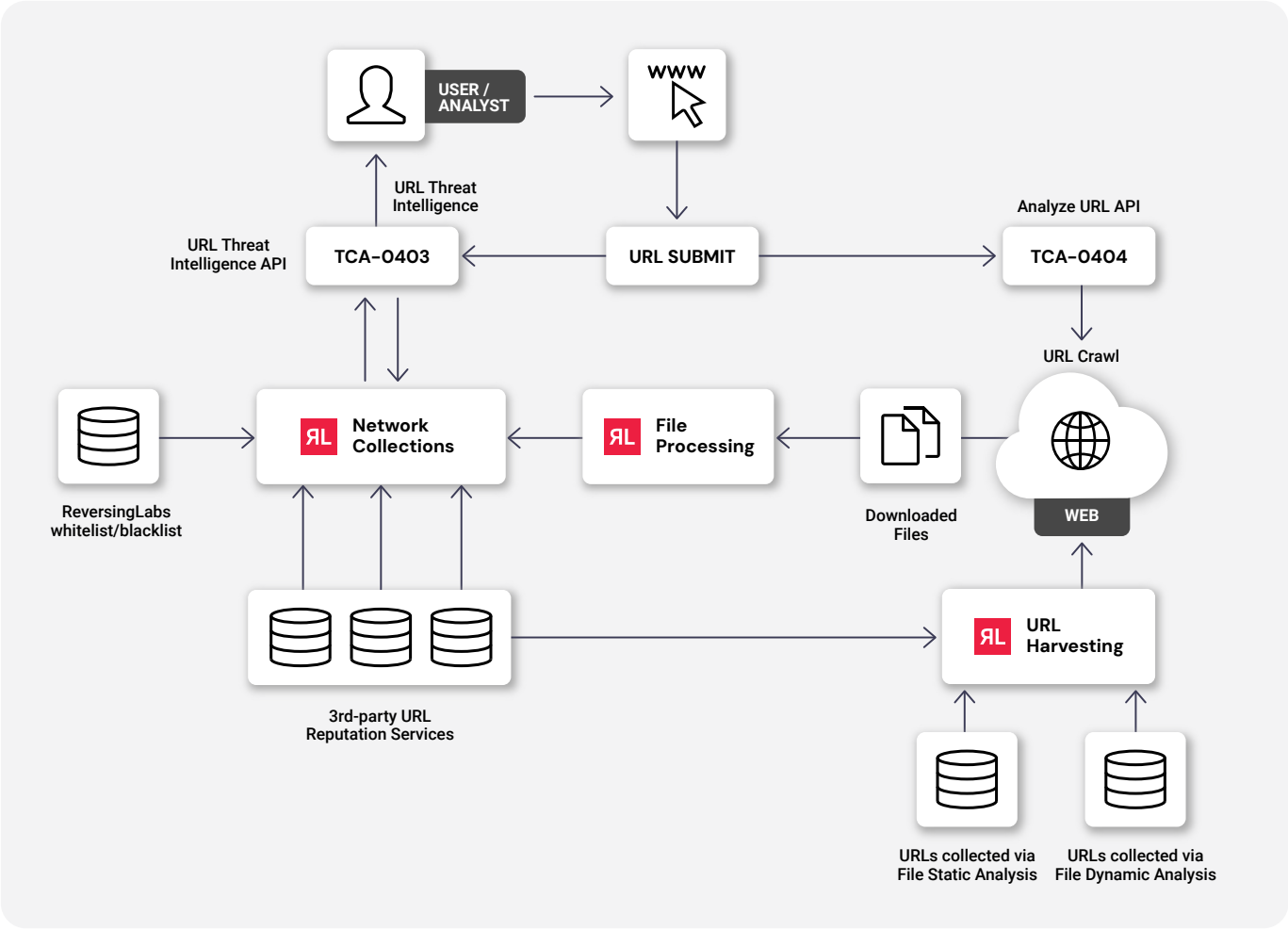
The service allows users to submit a URL for analysis. The analysis is a crawling process that will look for files to download from the submitted URL. When downloaded, the files are automatically sent for analysis to the ReversingLabs file processing pipeline for threat analysis.

Additional notes:

- Support for HTTP/HTTPS protocols
- URL analysis service supports redirects i.e. crawl will be performed on the final URL
- Files are downloaded only from the submitted URL, no recursion (crawl depth = 1)
- 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 the website/opendirectory
- Maximum of 50 samples per crawl
- Maximum size of each downloaded sample - 100 MB

Information when the analysis over the 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 crawl report, along with a list of samples downloaded from the submitted URL, can be retrieved via the TCA-0403 URL Threat Intelligence service.



©2024 ReversingsLabs All Right Reserved

TCA-0405 Domain Threat Intelligence

Similar to TCA-0403 URL Threat Intelligence, this service allows users to get a full threat intelligence report for the submitted Domain. It will provide a user with the report containing:

- **Third-party domain reputation and categorization** - ReversingLabs continually consults 15+ quality sources to get domain reputation
- **Reputation of files downloaded from a domain** - Counters of samples downloaded from the domain, mapped to their classification status (malicious, suspicious, known, unknown)
- **The most common threats** (malware type, family) found on the domain
- **Last DNS records**
- **Parent Domain information**

Additionally, through separated endpoints, the service provides insight into:

- **Files downloaded from a Domain** (with rich metadata and classification)
- **Related Domains** (provides a list of domains that have the same top parent domain as the requested domain)
- **URLs with this Internet Domain**
- **Resolutions** (domain-to-IP mappings captured when URLs with a given Domain were analyzed)

TCA-0406 IP Threat Intelligence

This service allows users to get threat intelligence for the submitted IP. It will provide a user with the full threat report containing:

- **Third-party IP address reputation** - ReversingLabs continually consults 10+ quality sources to get IP reputation
- **Reputation of files downloaded from an IP** - Counters of samples downloaded from the IP address, mapped to their classification status (malicious, suspicious, known, unknown)
- **The most common threats** (malware type, family) hosted on the submitted IP address

Additionally, through separated endpoints, a user will be able to get:

- **Files downloaded from a Domain** (with rich metadata and classification)
- **Related URLs** (a list of URLs hosted on the submitted IP address)
- **Resolutions** (IP-to-domain mappings captured when URLs hosted on the IP were analyzed)

TCA-0207/TCA-0106 RL Spectra Sandbox URL Analysis

The TCA-0207 service allows users to submit a URL for analysis in ReversingLabs Spectra Sandbox. By submitting a URL to the sandbox, a user can securely and safely open an untrusted website in a browser that runs in an isolated environment outside of the user's network. Using TCA-0106, a user can fetch a detailed report containing URL classification, signatures indicating detected malicious behavior such as phishing, and a wide range of other behavior data, including the document object model (DOM) tree, images, all HTML, JavaScript, etc. In addition, screenshots of the desktop as well as the full network data are captured.

TCA-0401 URI to Hash Search

The TCA-0401 service provides a list of all available file hashes associated with the requested URI (domain, IP address, email or URL) regardless of file classification. Results can be filtered by their classification (malicious, suspicious, known, unknown).

TCA-0402 URI Statistics

The TCA-0402 service provides statistical information on how many known, malicious, and suspicious samples are associated with a particular URI. The following URI types are supported: email, URL, IPv4 address, domain.

©2024 ReversingsLabs All Right Reserved

ReversingLabs Network Feeds

TCF-0301 Network IOCs Feed

The service offers **a continuous list of malicious URLs**. These are URLs from which ReversingLabs has downloaded malicious payloads or URLs identified as malicious by 20+ different reputation sources that ReversingLabs consults daily. Before entering the feed, URLs are checked against the internally curated whitelist to avoid benign and well-known sites being included.

TCTF-0001 Ransomware and Related Tools Intel Feed

The indicators selected for inclusion in this feed include both ransomware and malware related to ransomware attacks such as the malware used in the initial infection as well as lateral movement and data exfiltration. The indicators are vetted and designed to be directly actionable in TIPs and security products used in detection and prevention of malware.

Features of the feed include:

- **Indicators from multiple stages of typical attacks** allow for early detection and the ability to reduce damage associated with IP theft and ransomware attacks
- **Aggressive aging of the indicators** ensures only relevant indicators are active in the list
- **Extensive post processing of indicators** eliminates or reduces confidence on indicators likely to produce false positives
- **IP, Domain, and Hash indicators tagged with contextual data** such as malware family, network parameters, MITRE ATT&CK and attack progression stage
- **Direct integration into multiple TIP platforms and in STIX/TAXII format**

Get started!

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

REQUEST A DEMO

reversinglabs.com

About ReversingLabs

ReversingLabs is the trusted name in file and software security. We provide the modern cybersecurity platform to verify and deliver safe binaries. Trusted by the Fortune 500 and leading cybersecurity vendors, the ReversingLabs Spectra Core powers the software supply chain and file security insights, tracking over 40 billion searchable files daily with the ability to deconstruct full software binaries in seconds to minutes. Only ReversingLabs provides that final exam to determine whether a single file or full software binary presents a risk to your organization and your customer.

© Copyright 2024 ReversingLabs. All rights reserved. ReversingLabs is the registered trademark of ReversingLabs US Inc. All other product and company names mentioned are trademarks or registered trademarks of their respective owners.

REVERSINGLABS

Worldwide Sales +1.617.250.7518
sales@reversinglabs.com