REVERSINGLABS

ReversingLabs Network Threat Intelligence APIs & Feeds

Comprehensive network reputation, URL analysis, and threat intelligence

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

ReversingLabs Spectra Intelligence delivers this through a rich set of APIs and feeds, combining proprietary classification, ~50 third-party reputation sources, static and dynamic analysis, and curated threat feeds; all of this accessible via REST API.

ReversingLabs Network APIs

TCA-0407 Network Reputation

A fast, lightweight reputation verdict for any submitted URL, domain, or IP address. Ideal for real-time triage and automated decisioning in SOC workflows.

- **ReversingLabs classification (for URLs):** malicious, suspicious, known, or unknown. Including a detailed classification reason (e.g., file reputation, sandbox, third-party reputation, analyst override, blacklist/whitelist).
- **Third-party detection overview** from network threat intelligence partners.
- **URL categorization** (e.g., phishing, gambling, adult content) sourced from third-party providers and user overrides.
- **Threat severity score (0–5)** and threat name for malicious/suspicious indicators.
- **Associated malware indicator** showing whether malware samples have been found linked to the network location.
- **First seen / last seen timestamps** for historical tracking.
- Supports **single and bulk queries** (up to 100 records combining URLs, domains, and IPs per request).

Domain and IP queries return all fields except the ReversingLabs proprietary classification, which is URL-specific.

TCA-0408 Network Reputation Override

A fast, lightweight reputation verdict for any submitted URL, domain, or IP address. Ideal for real-time triage and automated decisioning in SOC workflows.

- Override any URL classification to **malicious, suspicious, or known**.
- Set custom **threat level, TTL (time-to-live), and categories** per override.
- **Remove overrides** in the same request.
- **List existing overrides** for audit and review.
- Supports **bulk operations**, up to 100 overrides and removals per request.

TCA-0404 Analyze URL

Comprehensive URL analysis combining static file analysis, dynamic behavioral assessment, network infrastructure mapping, and visual documentation to deliver complete threat intelligence. Supports three analysis workflows:

- **Full analysis (default)** — downloads content from the submitted URL and from URLs found on the page. Most comprehensive mode.
- **Light analysis** — downloads only content from the submitted URL, skipping linked content for faster results.
- **Fileless analysis** — skips content downloading entirely, focusing on URL reputation and infrastructure analysis. Ideal for high-volume triage.

Key capabilities:

- Downloads and analyzes **up to 50 samples per analysis** (each up to 100 MB), processed through the ReversingLabs threat detection pipeline.
- **DOM capture and analysis** to identify malicious JavaScript, hidden content, and dynamic page elements.
- **Page screenshots** for visual threat assessment and evidence collection.
- **DNS records, SSL/TLS certificate details**, and serving IP resolution for infrastructure analysis.
- **WHOIS domain registration and ownership data** for attribution and threat actor profiling.
- **Sandbox execution** in controlled environments to observe runtime behavior and detect evasive threats.
- **Full redirect chain** documentation and analysis at each step.
- **Supports HTTP/HTTPS protocols**; crawl depth = 1 (submitted URL only, no recursion).
- **Automatic re-crawls** to detect new malware versions or files deployed on the same URL.

Reports are retrieved via TCA-0403 URL Threat Intelligence. Downloaded samples typically reach full classification within ~30 minutes. The Notification Feed alerts when analysis is complete.

TCA-0403 URL Threat Intelligence

Returns a full threat intelligence report for any submitted URL, combining ReversingLabs proprietary classification, third-party reputation, static and dynamic analysis results, and file-level intelligence.

- **URL classification** based on the proprietary ReversingLabs algorithm that considers third-party reputation and the latest file reputation of all files downloaded across all analyses.
- **Third-party URL reputation and categorization:** ReversingLabs continually consults ~50 quality sources.
- **Static and dynamic analysis metadata** for each performed URL analysis, including sandbox detonation results (browser: Chrome), internet simulation settings, geolocation, and locale.
- **Downloaded file statistics** mapped to classification (malicious, suspicious, known, unknown) with risk score (0–10) and threat level (0–5).
- **Screenshots and DOM objects** captured during analysis for visual threat assessment and evidence.
- **Top threats** (malware family, type) downloaded from the URL.
- **Redirect chain tracking** with final URL, serving IP, hosting domain.
- **URL Analysis Notification Feed** is a continuous stream of URLs analyzed to completion.

Additionally provides endpoints for downloading file lists (with extended metadata and classification filtering), and supports bulk queries (up to 100 URLs per request).

TCA-0405 Domain Threat Intelligence

Returns a full threat intelligence report for any submitted domain, with reputation data, file statistics, DNS records, SSL/TLS certificates, and related domain/URL context.

- **Third-party domain reputation and categorization:** ReversingLabs continually consults 15+ quality sources.
- **Downloaded file statistics** mapped to classification (malicious, suspicious, known, unknown).
- **Top threats** (malware type, family) found on the domain.
- **Last DNS records** with change timestamps.
- **SSL/TLS certificate data** including validity dates, signature algorithm, issuer, common name, serial number, thumbprints (MD5, SHA1, SHA256), and certificate extensions per port.
- **Parent domain information**.
- **First seen / last seen timestamps** for historical tracking.

Additional endpoints: files downloaded from the domain (with rich metadata), related domains (subdomains/siblings sharing the same top parent domain), related URLs hosted on the domain, and domain-to-IP resolution mappings. Bulk queries supported (up to 100 domains per request).

TCA-0406 IP Threat Intelligence

Returns a full threat intelligence report for any submitted IP address, with reputation data, file statistics, WHOIS ownership, and GeoIP enrichment.

- **Third-party IP address reputation:** ReversingLabs continually consults 15+ quality sources.
- **Downloaded file statistics** mapped to classification (malicious, suspicious, known, unknown).
- **Top threats** (malware type, family) hosted on the IP.
- **WHOIS registration and ownership data** available via the extended parameter for attribution and investigation.
- **GeoIP enrichment** with AS number, AS organization, network CIDR, city, country, latitude/longitude.
- **First seen / last seen timestamps.**

Additional endpoints: files downloaded from the IP (with rich metadata and classification filtering), related URLs hosted on the IP, and IP-to-domain resolution mappings. Bulk queries supported (up to 100 IPs per request).

TCA-0207 RL Spectra Sandbox URL Analysis

Submit URLs for dynamic analysis in the ReversingLabs Cloud Sandbox. URLs are opened in a browser within an isolated environment, and a detailed report containing classification, behavioral signatures, DOM tree, screenshots, JavaScript analysis, and full network capture is generated.

- **Multi-platform sandbox environments:** Windows 11, Windows 10, Windows 7, macOS 11, Linux.
- **URL and file detonation** with full behavioral observation.

The full dynamic analysis report (including phishing signatures, DOM tree, HTML/JavaScript analysis, desktop screenshots, full network traffic (PCAP), memory strings, dropped files, and YARA rule matches) is available via the TCA-0106 Dynamic Analysis Report API.

TCA-0401 URI to Hash Search

Returns a list of all SHA1 file hashes associated with a requested URI (domain, IP address, email, or URL). Hashes are identified through static analysis of file contents (i.e., files found to contain the requested URI during processing). Results can be filtered by classification (malicious, suspicious, known, unknown). This provides a unique correlation between network indicators and the files that reference them.

TCA-0402 URI Statistics

Provides statistical information on how many known, malicious, and suspicious samples are associated with a particular URI. Leverages network IOCs extracted during file static analysis to correlate URIs with samples. Supported URI types: email, URL, IPv4 address, and domain.

ReversingLabs Network Feeds

TCF-0301 Network IOCs Feed

A continuous stream of malicious URLs identified by Spectra Intelligence, sourced from URLs delivering malicious payloads and from ~50 third-party reputation sources consulted daily. All entries are checked against an internally curated whitelist to suppress benign and well-known sites.

- **Malicious URL indicators** — URLs confirmed as delivering malware or flagged by multiple reputation sources.
- **File metadata for delivery URLs** — when a URL is observed delivering malicious files, the feed includes the SHA1 hash, SHA256, and the ReversingLabs threat name of the downloaded payload.
- **Whitelist-filtered** — internally curated suppression list reduces noise from known-good infrastructure.

TCTF-0001 Ransomware Feed

Focused exclusively on ransomware, made up of files, C2 infrastructure, and payload delivery URLs, all drawn from a pipeline processing ~20 million samples per day. Only high-confidence indicators are included, significantly reducing false positives compared to broader feeds.

- **Ransomware-associated files** — identified and classified through static and dynamic analysis.
- **C2 infrastructure** — command-and-control addresses extracted directly from malware configurations.
- **Payload delivery URLs** — distribution points observed in active ransomware campaigns.
- **Rich IOC context** — each indicator is enriched with threat names, malware families, attack stages, MITRE ATT&CK techniques, and threat actor associations.

Delivered via STIX 2.1 / TAXII 2.1. Integrates with major SIEM, SOAR, EDR, and TIP platforms.

Full API reference & OpenAPI specification: docs.reversinglabs.com/SpectraIntelligence
Python SDK: pypi.org/project/reversinglabs-sdk-py3

Common Use Cases for Enterprise Defenders

Malware Detection Feed (Platform Filtered)

When an analyst or SIEM alert surfaces a suspicious URL, domain, or IP, use **TCA-0407** for an instant reputation verdict (malicious, suspicious, known, or unknown) without triggering a full analysis. Supports bulk queries of up to 100 mixed indicators per request, enabling automated triage pipelines at scale.

Deep Investigation of Suspicious URLs

Submit a suspected phishing or malware-delivery URL via **TCA-0404** (Analyze URL), then retrieve the full report through **TCA-0403**. Results include DOM capture, screenshots, downloaded file classifications, redirect chains, and sandbox detonation; giving analysts everything needed for escalation or case closure.

Domain & IP Profiling for Threat Hunting

Use **TCA-0405** and **TCA-0406** to build a full threat profile of a domain or IP including top malware families hosted, DNS history, SSL/TLS certificates, WHOIS ownership, GeoIP context, and related infrastructure. Ideal for pivot-based hunting when one IOC leads to an entire threat actor's infrastructure.

Correlating Network IOCs with Malware Samples

When investigating a C2 domain or malicious URL, use **TCA-0401** (URI-to-Hash Search) to find all malware samples that reference it, extracted via static analysis of file contents. Pair with **TCA-0402** (URI Statistics) to understand the volume and severity of associated samples before prioritizing a deeper file investigation.

Managing False Positives Across the Organization

Use **TCA-0408** to override URL classifications organization-wide to mark internal tools or partner sites as known, or flag undetected threats as malicious. Overrides propagate to all users within the account, ensuring consistent verdicts in SIEM, SOAR, and proxy enforcement downstream.

Automating Feed Ingestion into SIEM/TIP Platforms

Ingest **TCF-0301** (Network IOCs) and **TCTF-0001** (Ransomware Feed) directly into platforms like Microsoft Sentinel, OpenCTI, or Splunk via STIX 2.1 / TAXII 2.1. Curated, high-confidence indicators with ATT&CK mappings and threat actor context arrive ready for automated detection rule generation and alert enrichment, no manual processing required.

Get started!

Improve your detection efficacy with high-fidelity, validated threat intelligence and threat classifications you can trust.

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, RL Spectra Core powers the software supply chain and file security insights, tracking over 450 billion searchable files 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 customers.

Rev-DS-07.01.26

REVERSINGLABS

Worldwide Sales +1.617.250.7518
sales@reversinglabs.com