# Malware Intelligence, Enrichment APIs and Feeds for ThreatStream

File-level malware details instantly available with one click

## Key Solution Highlights

- **THREAT INTELLIGENCE FEEDS. ReversingLabs Titanium Platform provides feeds of high-quality malware indicators, enriching Anomali ThreatStream with powerful investigation and classification tools so SOC Analysts can instantly identify malware.**
- **ACTIONABLE MALWARE ENRICHMENT. The ReversingLabs solution displays malware context, identifying file type, capabilities, and additional related indicators enabling threat hunters to pivot on details and enforce rapid containment.**
- **DETECT EMERGING THREATS. ReversingLabs feeds can be delivered via ThreatStream and directed to a SIEM or other detection tools to identify malware and detect emerging threats.**

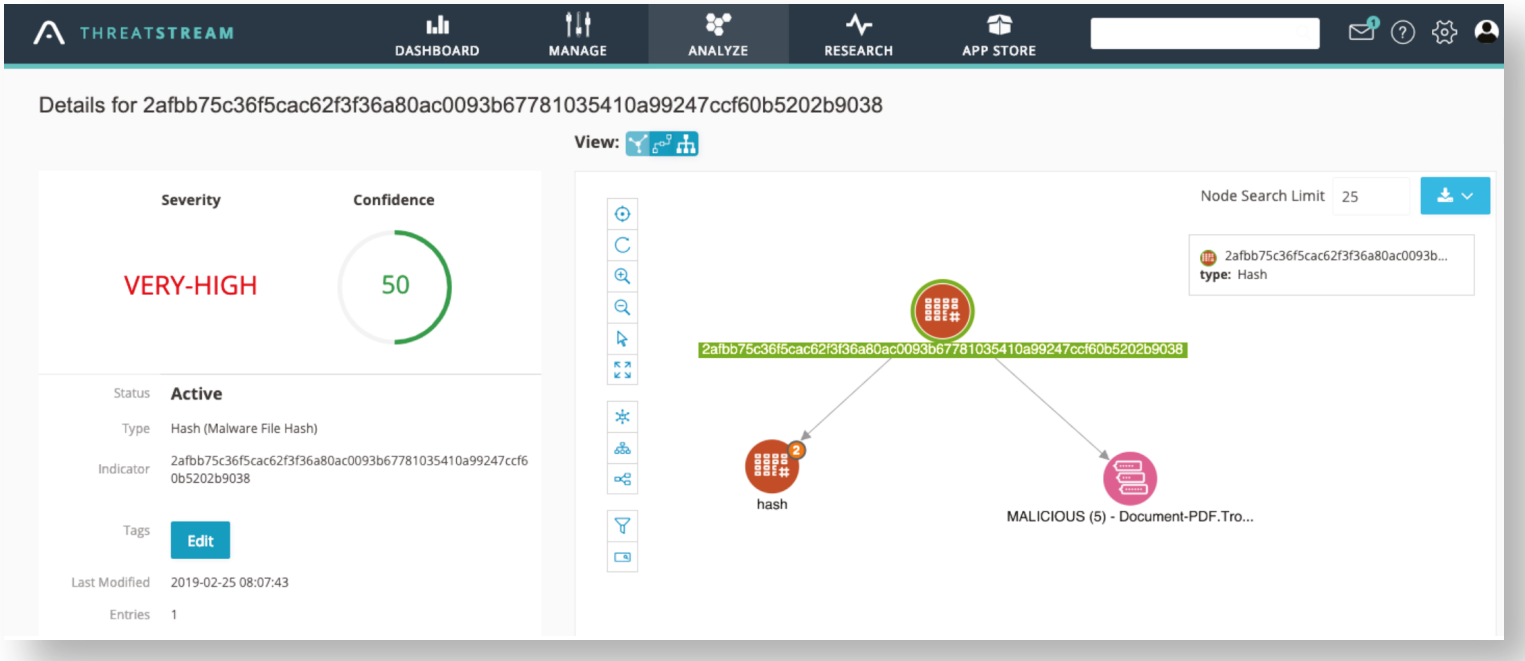
## Joint ReversingLabs & Anomali Solution Value

The cybersecurity threat intelligence market has the potential to keep organizations ahead of advanced malware by using the latest threat data to update security devices to prevent compromise. However, massive volumes of data aggregated from various feeds, lack of analysts, and unknown polymorphic malware challenges organizations from containing malware. Without actionable threat intelligence, SOC analysts and threat hunters are challenged to find malware before it executes, forcing them to waste already limited resources and time piecing together malware indicators from disparate sources.

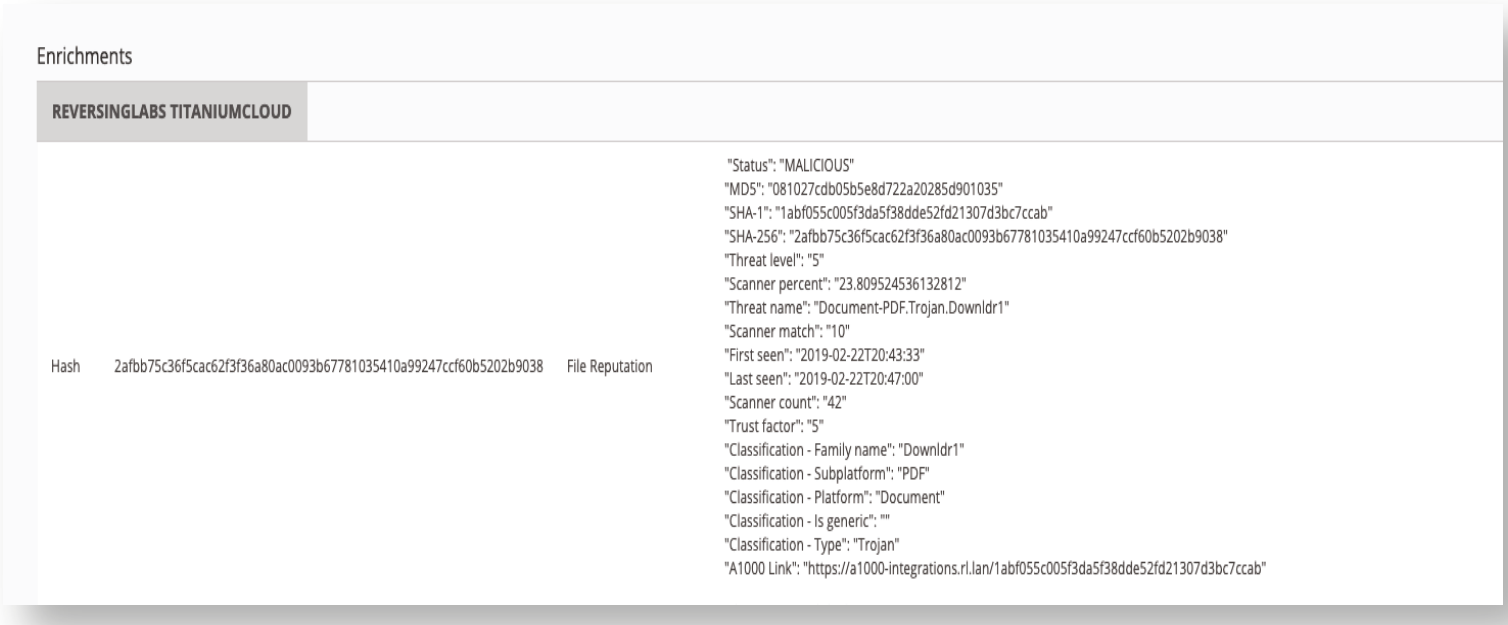
To address this problem, Anomali ThreatStream aggregates, optimizes and manages cyber threat intelligence with their platform, providing a complete picture of an organizations threat intelligence posture. ReversingLabs enriches Anomali ThreatStream with file analysis and detailed malware indicators from the authoritative global reputation database of over 10 billion files for accelerated SOC response. The ReversingLabs Titanium Platform service displays malware details and context in ThreatStream so threat hunters can investigate hashes and URLs to understand threat capabilities instantly.

The ReversingLabs plug-and-play APIs and Feeds are integrated with Anomali ThreatStream and connect with existing SOC Analyst workflows to automate and simplify much of the malware detection and analysis work traditionally done themselves. For preventive security, threat hunters can use the enriched malware details to automatically feed SIEM, FW, IPS and EDR for matching incoming files against lists of indicators to find malware instantly or to push found indicators directly to blacklists.

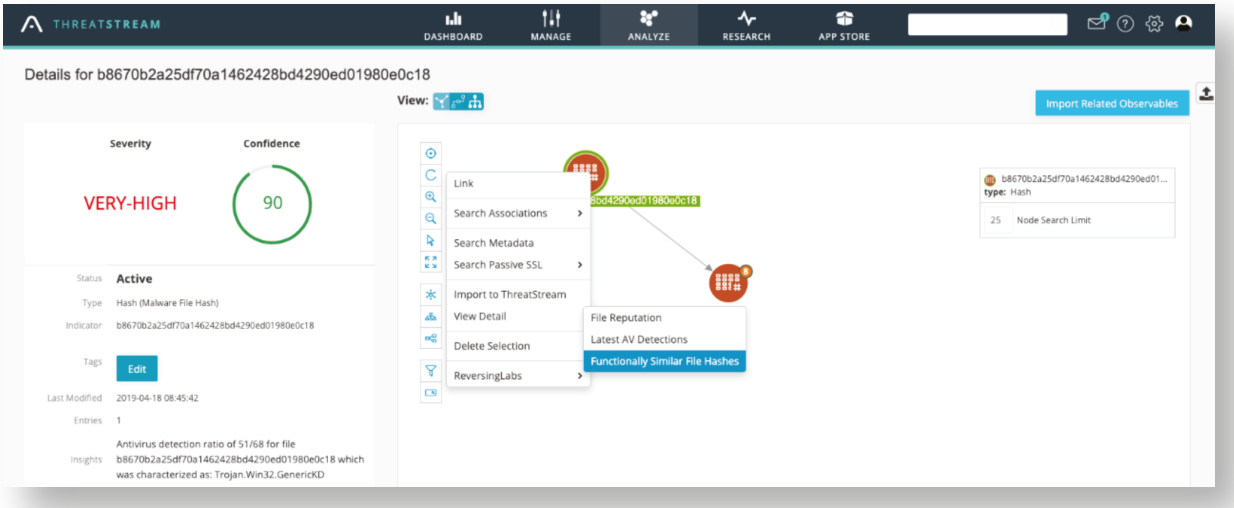
**Hash Enrichment with File Reputation Analysis** (TCA-0101) of instant Malware Severity Level + 'Malicious', 'Suspicious' or 'Known Good' classification and a collection of alternate hashes (SHA-1, MD5, SHA-256 and others) to enable rapid detection across the entire security ecosystem.

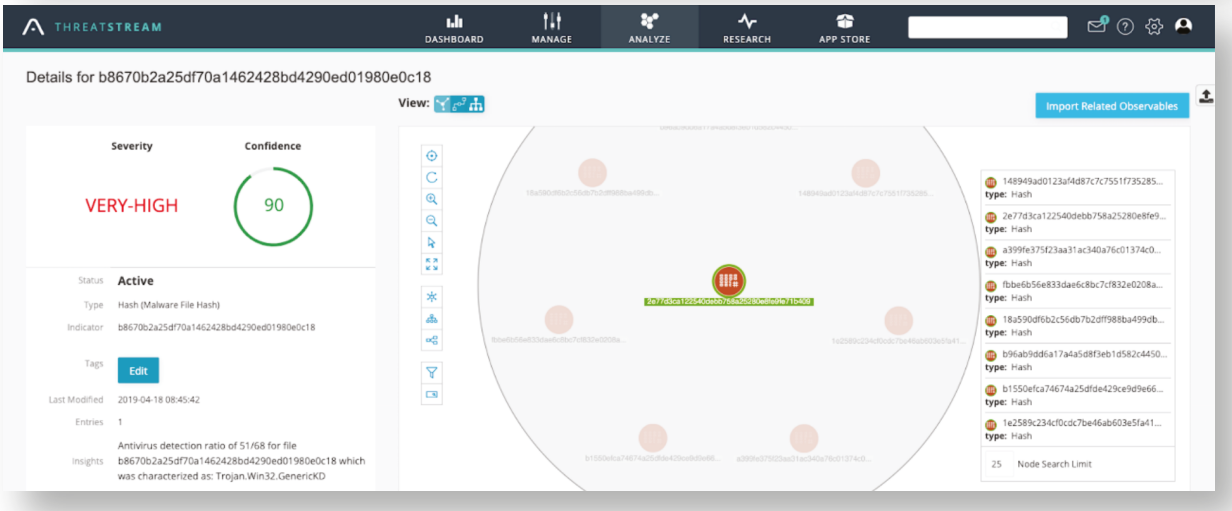



**Hash Enrichment with Multi-AV Scan Detection Results** (TCA-0103) for objects tracked in Anomali ThreatStream, to enable correlation and rapid response to emerging threats.

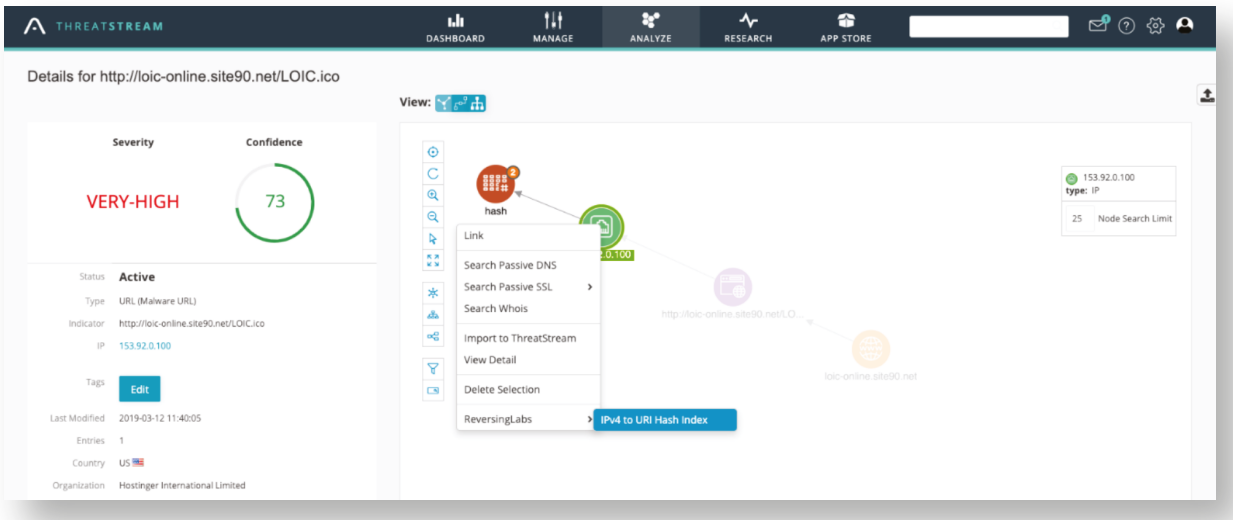


**SHA1 Enrichment with Functionally Similar Malware Hashes** (TCA-0301) to identify malware samples with related structure and behavior, providing a powerful technique to detect evasive malware.




**URL Enrichment with Malicious File Hashes** (TCA-0401) to query the TitaniumCloud database for known malicious file hashes associated with a domain or IP address.



# How It Works

- ReversingLabs offers API's for file-based malware threat intelligence, and premium enrichment feeds that allow you to pull the latest global detection results directly into Anomali ThreatStream.
- Evaluate and purchase from the Anomali App Store:
    - Login to Anomali ThreatStream,
    - Go to the Anomali APP Store and request a trial version of ReversingLabs APIs and Feeds to try it out for yourself. There are two ways to try at no cost:
        1. ReversingLabs File Intelligence Evaluation Bundle
        2. ReversingLabs TitaniumCloud Threat Intelligence ELMA Feed

# ReversingLabs Solution Components

Titanium Platform **APIs** for Anomali ThreatStream Enrichment with file and URL intelligence to investigate threats:

- **File Reputation** - TCA-0101. File reputation from the authoritative cloud source allowing rapid identification and detection. The API provides classification for malware and goodware, threat type and severity, first-seen and last-seen date, alternate hashes of the same binary, and summary of Anti Virus detections.
- **Anti Virus Detections** - TCA-0103. The most recent cloud Anti Virus scan results with vendor, threat name, scan date provides useful pivoting data for actionable correlation and investigation intelligence.
- **Functionally Similar Malware Hunting** - TCA-0301. Pivot from SHA-1 hash to functionally-similar malware within known malware families using RHA (ReversingLabs Hashing Algorithm).
- **URI to Hash Search** - TCA-0401. Find malware hashes associated with URLs, IP addresses, domains, or emails.

Titanium Platform **ELMA Feeds** of new file hashes that we've found in the wild, and are updated hourly with a downloadable report for more details for Anomali ThreatStream:

- **New Exploit/CVE Samples** (TCF-0203)
- **New Linux Malware** (TCF-0104)
- **New MacOS Malware** (TCF-0103)
- **New Android Malware** (TCF-0102)

Additionally, you can submit hashes to the **A1000 Threat Analysis and Hunting Workbench** for further malware investigation.

# About ReversingLabs

ReversingLabs is the leading provider of explainable threat intelligence solutions that dissect complex file-based threats for enterprises stretched for time and expertise. Its hybrid-cloud Titanium Platform enables digital business resiliency, protects against new modern architecture exposures, and automates manual SOC processes with a transparency that arms analysts to confidently take action and hunt threats.

# About Anomali

Anomali® delivers intelligence-driven cybersecurity solutions, these include Anomali ThreatStream®, Anomali Match™, and Anomali Lens™. Private enterprises and public organizations use Anomali to gain unlimited visibility, speed time to detection, and constantly improve security operations. Anomali customers include more than 1,500 global organizations, many of the Global 2000 and Fortune 500, and large government and defense organizations around the world. Founded in 2013, it is backed by leading venture firms including GV, Paladin Capital Group, Institutional Venture Partners, and General Catalyst. Learn more at: www.anomali.com



REVERSINGLABS

**Worldwide Sales : +1.617.250.7518**
**sales@reversinglabs.com**