REVERSINGLABS

Actionable Malware Intelligence for Anomali ThreatStream

Trusted Reputation Data, Deep Malware Insights, High-Value Enrichment

Joint ReversingLabs & Anomali Solution

High-fidelity threat intelligence that's timely and contextual can mean the difference between thwarting a costly cyber-attack instead of having to recover from one. Without threat intelligence that's trusted and actionable, analysts and threat hunters are at a significant disadvantage to find destructive malware before it executes, forcing them to waste already limited resources and time researching, validating, and piecing together threat indicators from disparate sources. Combine this with a rise in polymorphic malware and advanced evasion techniques, it's no surprise that organizations are struggling to stay ahead of sophisticated cybercriminals.

With the joint ReversingLabs and Anomali solution, SOC teams can take advantage of actionable malware intelligence and valuable indicator enrichment from ReversingLabs within the Anomali ThreatStream platform. This integration empowers users with the most up-to-date file and network reputation data, along with context-rich threat intelligence from ReversingLabs' authoritative repository of malware and goodware, consisting of more than 400 billion samples, with millions of new samples added daily.

ReveringLabs adds meaningful context and verified threat details for file hashes, URLs, domains, and IPs, enabling security analysts and threat hunters to quickly investigate and understand threat capabilities in order to take fast and decisive action.

Solution Highlights

- **VETTED THREAT INTELLIGENCE**
  ReversingLabs delivers high-quality, validated malware indicators with contextually relevant information to accelerate analysis, investigations, and response.
- **AUTHORITATIVE REPUTATION DATA**
  ReversingLabs provides the most trusted and up-to-date file and network reputation data from its authoritative global data corpus, consisting of 400+ billion malware and goodware samples.
- **EMERGING THREAT DETECTION**
  ReversingLabs provides continuous coverage of emerging malware threats, including new CVE exploits in-the-wild, along with new threats unique to Linux, MacOS, and Android.
- **CURATED RANSOMWARE FEED**
  ReversingLabs' Ransomware Feed specifically targets the most prevalent ransomware families and provides vigorous curation of indicators to ensure only pertinent threats remain active in the list.

How It Works

The ReversingLabs app for Anomali ThreatStream is a set of pivot and context-based enrichment functions for files, URLs, domains, and IP addresses.

Pivot-Based Enrichments

Pivot-based enrichments are used to dynamically trigger actions over various types of observables. Each type of observable displays only actions that were made for its specific type.

Example: Leverage ReversingLabs to quickly identify malware samples with related structure and behavior, providing a powerful technique to detect evasive malware.

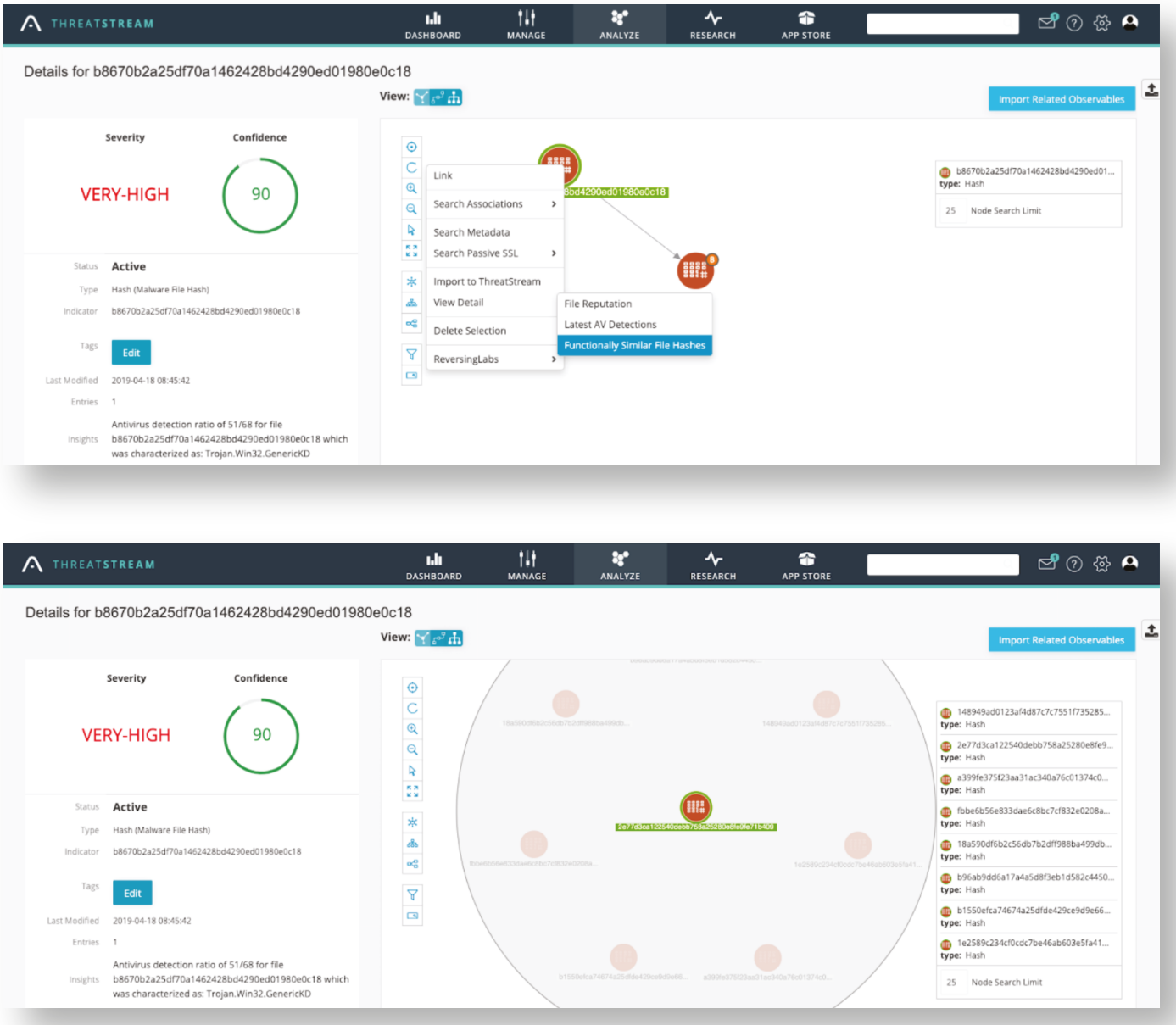

Figure 1 and 2: ReversingLabs' pivot-based enrichment displaying functionally similar malware.

Context-Based Enrichments

Context-based enrichments are displayed automatically when starting an observable investigation. Depending on the observable type, for instance a file hash versus URL, different enrichment tabs will be shown.

Example: ReversingLabs adds crucial context to aid in investigations, including reputation status, threat classification details, first seen/last seen dates, AV scanner results, and other valuable metadata.

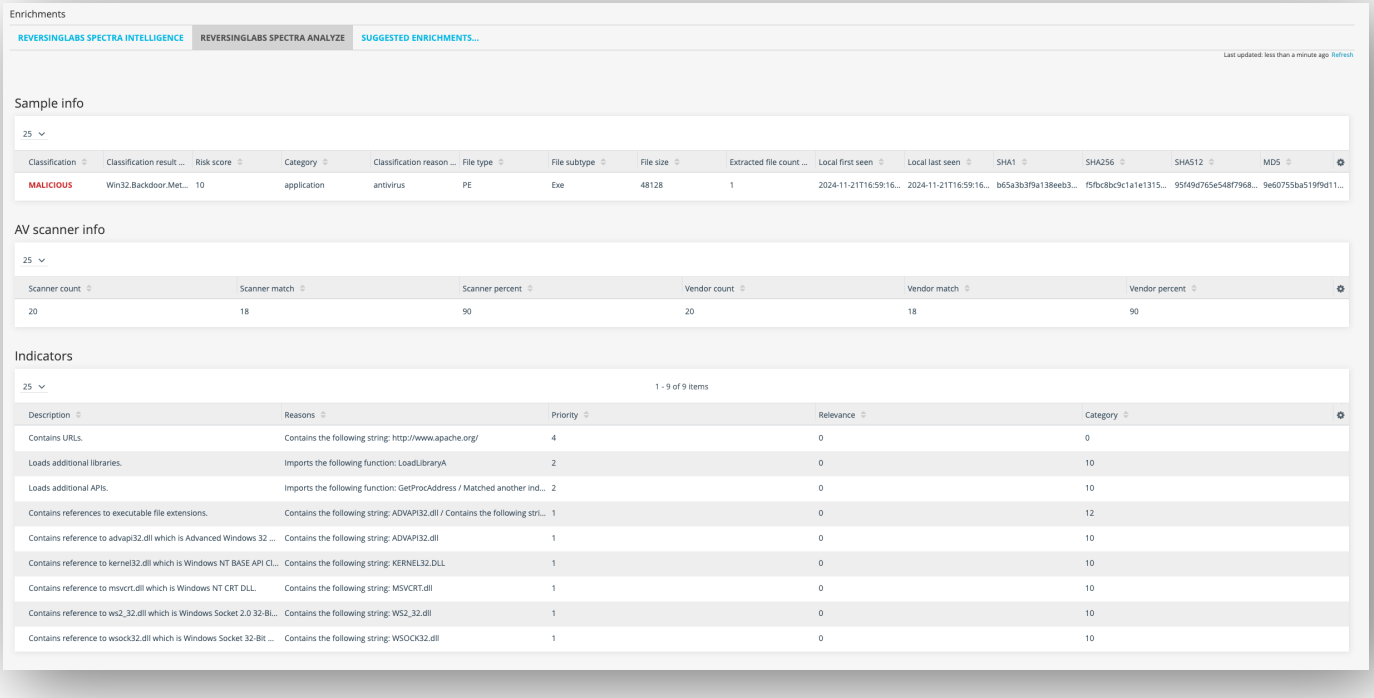

Figure 3: ReversingLabs' context-based enrichment for a file hash.

Try it for free!

Go to the Anomali APP Store and request a trial version of ReversingLabs APIs and Feeds to try it out for yourself.

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 422 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.

PB-Rev-06.04.25

REVERSINGLABS

Worldwide Sales: +1.617.250.7518
sales@reversinglabs.com