AL AEVERSINGLABS

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.

A THREATS	TREAM	DASHBOARD	MANAGE	analyze	↓ RESEARCH	APP STORE	⊴ ⊘ ⊛	
Details for b	3670b2a25df70a1462428bd4290ed01980e	0c18 View: <mark>⋎∕</mark> ₆ ° <mark>ਜ</mark> ி					Import Related Observables	
VE	Severity Confidence RY-HIGH 90	C C C Link Search As Search M	sociations >	8504290ed01980e0c18	b8670b2a25df70a1462428bd4290ed01 typet: Hath 25 Node Search Limit			
Status Type Indicator	Active Hash (Malware File Hash) b8670b2a25df70a1462428bd4290ed01980e0c18	× Search Pa ★ Import to & View Deta	ThreatStream	File Reputation				
Tags Last Modified	Edit 2019-04-18 08:45:42	Celete Se Reversing	Labs >	Functionally Similar Fil	e Hashes			
Entries	1 Antivirus detection ratio of 51/68 for file b8670b2a25df70a1462428bd4290ed01980e0c18 which was characterized as: Trojan.Win32.GenericKD							
Entries	1 Antivirus detection ratio of 51/68 for file b8670b2a25df70a1462428bd4290ed01980e0c18 which was characterized as: Trojan.Win32.GenericKD	_	_		_			



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.

Enrichments														
REVERSINGLABS SPI	ECTRA INTELLIGENCE	REVERSINGLABS SP	PECTRA ANALYZE	SUGGESTED ENRICHME	NTS									
		REFERENCES OF ST	LEHNTMERLE										Last updat	ed: less than a minute ago Refres
Sample info														
25 🗸														
Classification 🔅	Classification result	Risk score 🔅	Category 0	Classification reason	File type 🔅	File subtype 🔅	File size 🔅	Extracted file count	Local first seen 🔅	Local last seen 🔅	SHA1 0	SHA256 \$	SHA512 \$	MDS 0
MALICIOUS	Win32.Backdoor.Met	10	application	antivirus	PE	Exe	48128	1	2024-11-21T16:59:16	2024-11-21T16:59:16	b65a3b3f9a138eeb3	f5fbc8bc9c1a1e1315	95f49d765e548f7968.	. 9e60755ba519f9d11
AV scappor inf														
Av scanner inn	0													
25 ~														
Scanner count 🔅		Scanner m	hatch 🗘	Scanner percent 👙		Vendor count 单		dor count 🗘	Vendor match 🔅			Vendor percent 🕀		٥
20	18		90			20		18			90			
Indicators														
25 🗸							1 - 9 of 9 iter	ns						
Description 🗘			Reasons ≑			Priority 🗘			Relevance 🗘			Category 🗘		٥
Contains URLs.			Contains the followin	ng string: http://www.apach	ie.org/	4			0			0		
Loads additional lib	oraries.		Imports the following	g function: LoadLibraryA		2			0			10		
Loads additional AP	PIS.		Imports the following	g function: GetProcAddress	/ Matched another ind.	. 2			0			10		
Contains references	s to executable file extens	ions.	Contains the followin	ng string: ADVAPI32.dll / Co	ntains the following stri.	. 1			0			12		
Contains reference	to advapi32.dll which is A	dvanced Windows 32	Contains the followin	ng string: ADVAPI32.dll		1			0			10		
Contains reference	to kernel32.dll which is W	indows NT BASE API Cl	. Contains the followin	ng string: KERNEL32.DLL		1			0			10		
Contains reference	to msvcrt.dll which is Win	dows NT CRT DLL.	Contains the followin	ng string: MSVCRT.dll		1			0			10		
Contains reference	to ws2_32.dll which is Wir	ndows Socket 2.0 32-Bi	Contains the followin	ng string: WS2_32.dll		1			0			10		
Contains reference	to wsock32.dll which is W	indows Socket 32-Bit	Contains the followin	ng string: WSOCK32.dll		1			0			10		

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.



© Copyright 2025 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.

PB-Rev-06.04.25

Worldwide Sales: +1.617.250.7518 sales@reversinglabs.com