REVERSINGLABS ANOMALI™

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 to detect emerging threats.**

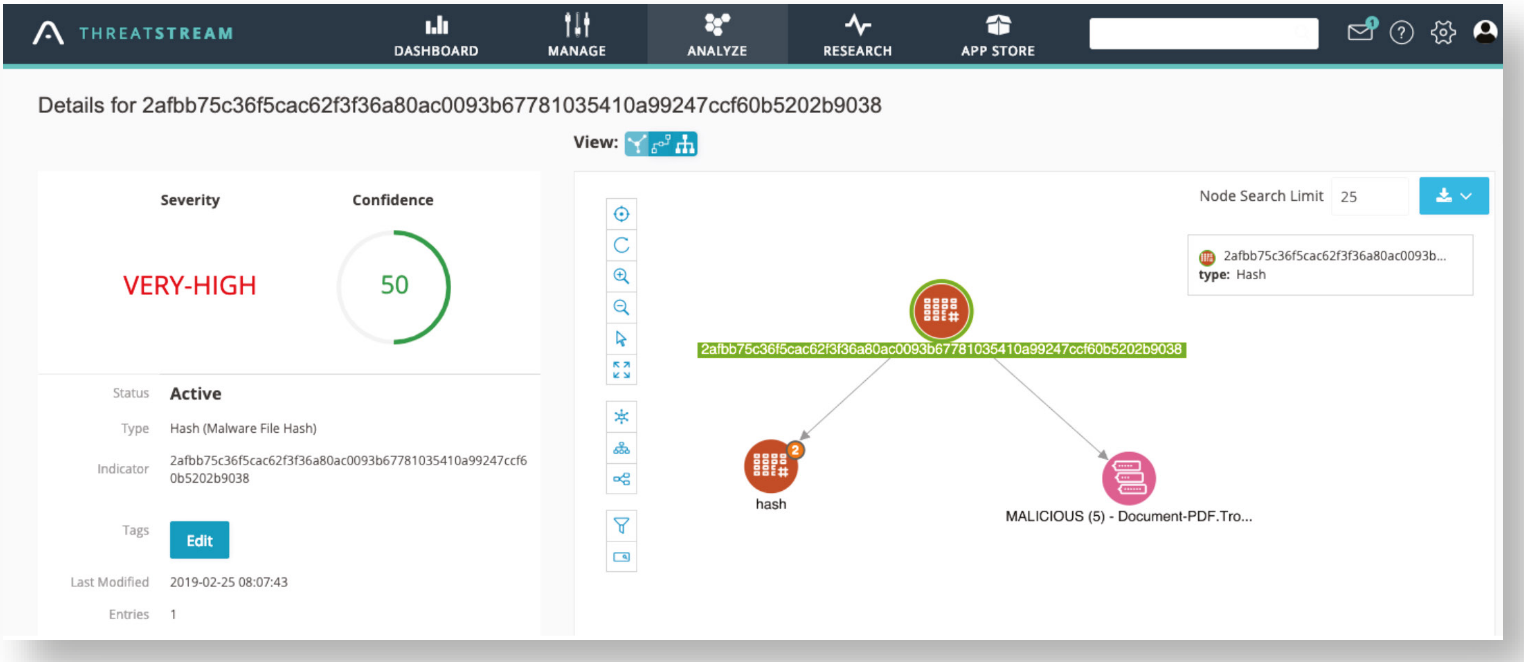
Joint ReversingLabs & Anomali Solution Value

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 8 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 EDRs for matching incoming files against lists of indicators to find malware instantly or to push found indicators directly to blacklists.

1. Display 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 and SHA-256) to enable rapid detection across diverse security tools.

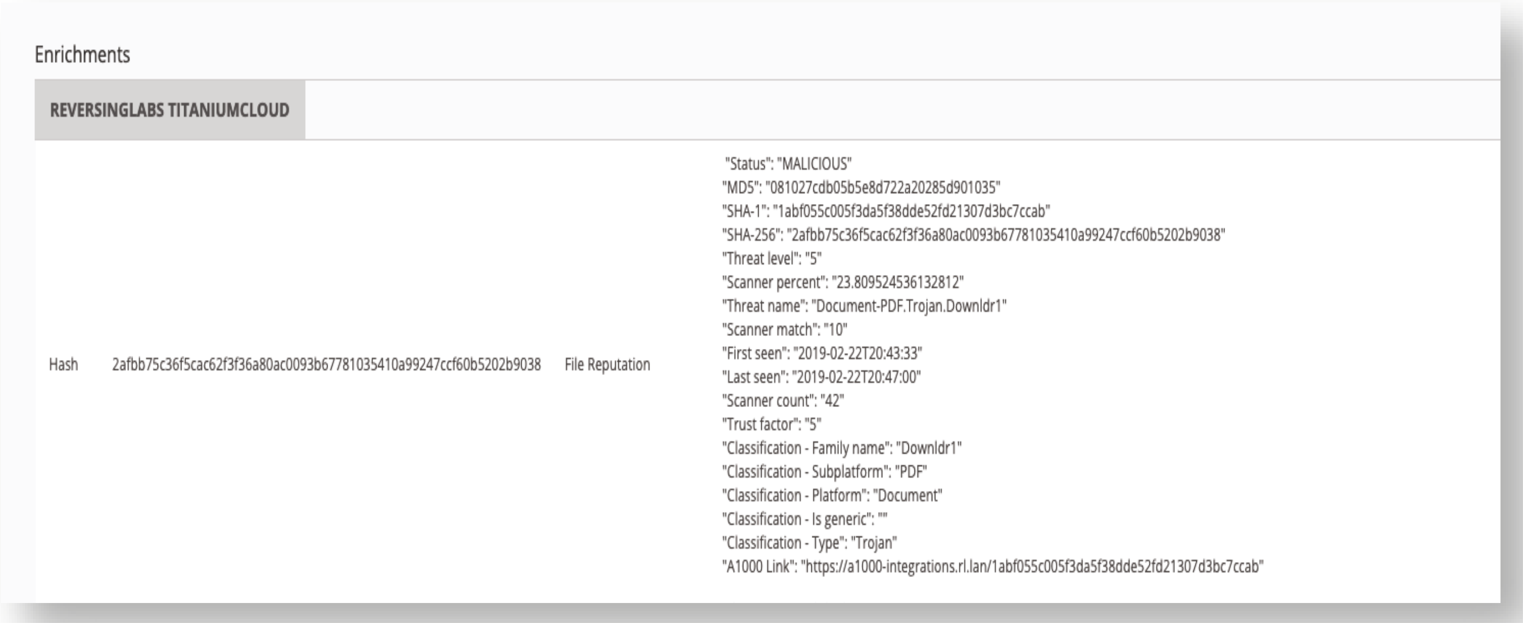

THREATSTREAM
DASHBOARD
MANAGE
ANALYZE
RESEARCH
APP STORE
View:
Node Search Limit
25
2afbb75c36f5cac62f3f36a80ac0093b...
type: Hash
2afbb75c36f5cac62f3f36a80ac0093b67781035410a99247ccf60b5202b9038
2
hash
MALICIOUS (5) - Document-PDF.Tro...

Details for 2afbb75c36f5cac62f3f36a80ac0093b67781035410a99247ccf60b5202b9038

Severity	Confidence
VERY-HIGH	50

Status	Active
Type	Hash (Malware File Hash)
Indicator	2afbb75c36f5cac62f3f36a80ac0093b67781035410a99247ccf60b5202b9038
Tags	Edit
Last Modified	2019-02-25 08:07:43
Entries	1

2. Display Hash Enrichment with Multi-AV Scan Detection Results (TCA-0103) for objects tracked in Anomali ThreatStream, helping rapid understanding of emerging threats.

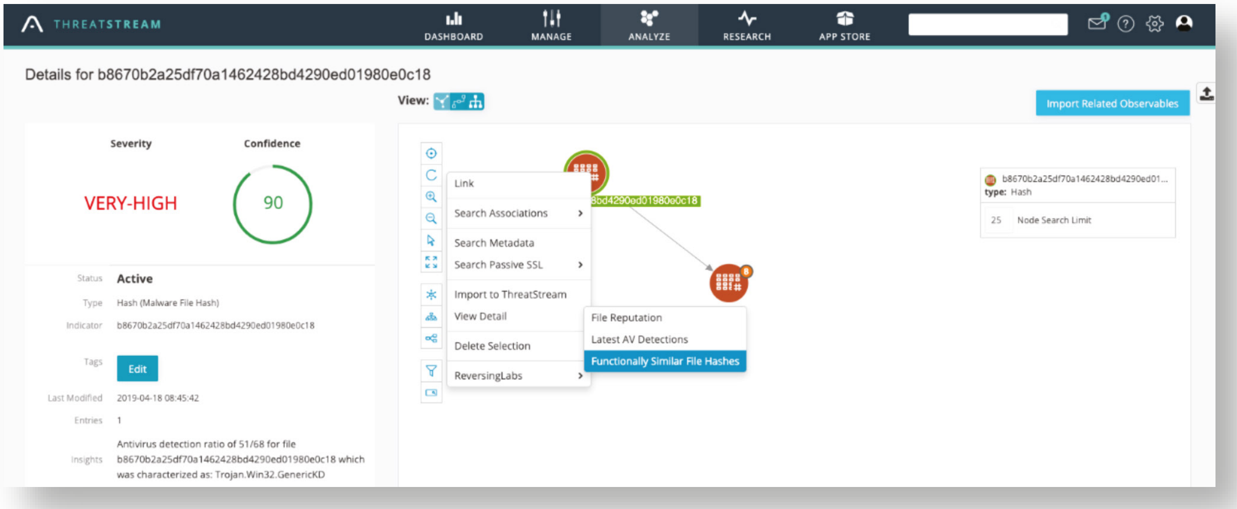


Enrichments

REVERSINGLABS TITANIUMCLOUD

Hash	2afbb75c36f5cac62f3f36a80ac0093b67781035410a99247ccf60b5202b9038	File Reputation	"Status": "MALICIOUS" "MD5": "081027cdb05b5e8d722a20285d901035" "SHA-1": "1abf055c005f3da5f38dde52fd21307d3bc7ccab" "SHA-256": "2afbb75c36f5cac62f3f36a80ac0093b67781035410a99247ccf60b5202b9038" "Threat level": "5" "Scanner percent": "23.809524536132812" "Threat name": "Document-PDF.Trojan.Downldr1" "Scanner match": "10" "First seen": "2019-02-22T20:43:33" "Last seen": "2019-02-22T20:47:00" "Scanner count": "42" "Trust factor": "5" "Classification - Family name": "Downldr1" "Classification - Subplatform": "PDF" "Classification - Platform": "Document" "Classification - Is generic": "" "Classification - Type": "Trojan" "A1000 Link": "https://a1000-integrations.rl.lan/1abf055c005f3da5f38dde52fd21307d3bc7ccab"

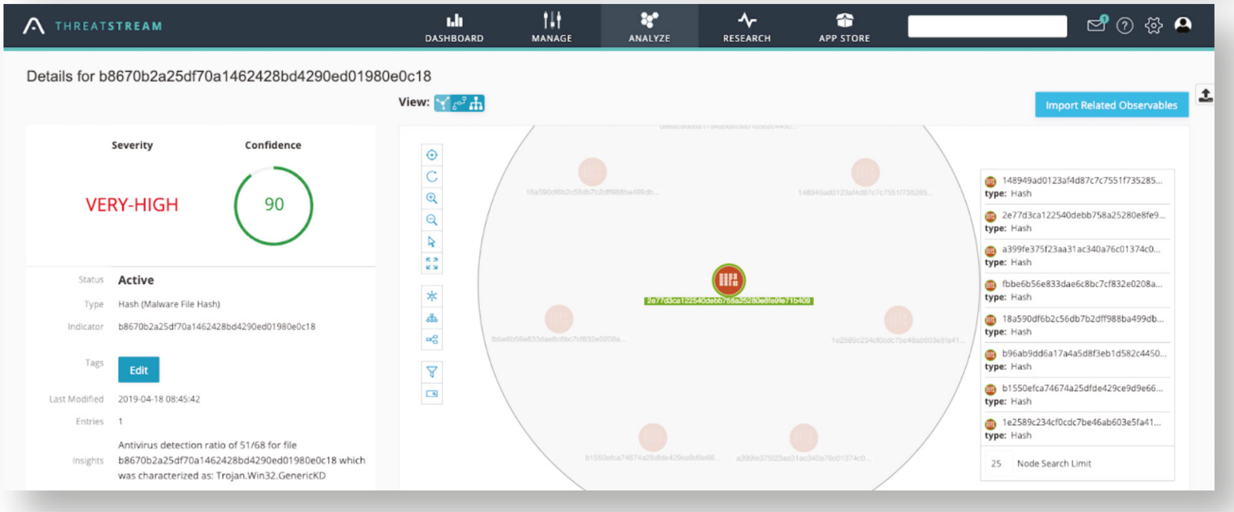
3. **Display SHA1 Enrichment with Functionally Similar Malware Hashes** (TCA-0301) to identify malware samples with related structure and behavior, providing a powerful technique to detect evasive malware.



Details for b8670b2a25df70a1462428bd4290ed01980e0c18

Severity: VERY-HIGH
Confidence: 90

Status: Active
Type: Hash (Malware File Hash)
Indicator: b8670b2a25df70a1462428bd4290ed01980e0c18
Tags: Edit
Last Modified: 2019-04-18 08:45:42
Entries: 1
Insights: Antivirus detection ratio of 51/68 for file b8670b2a25df70a1462428bd4290ed01980e0c18 which was characterized as: Trojan.Win32.GenericKD



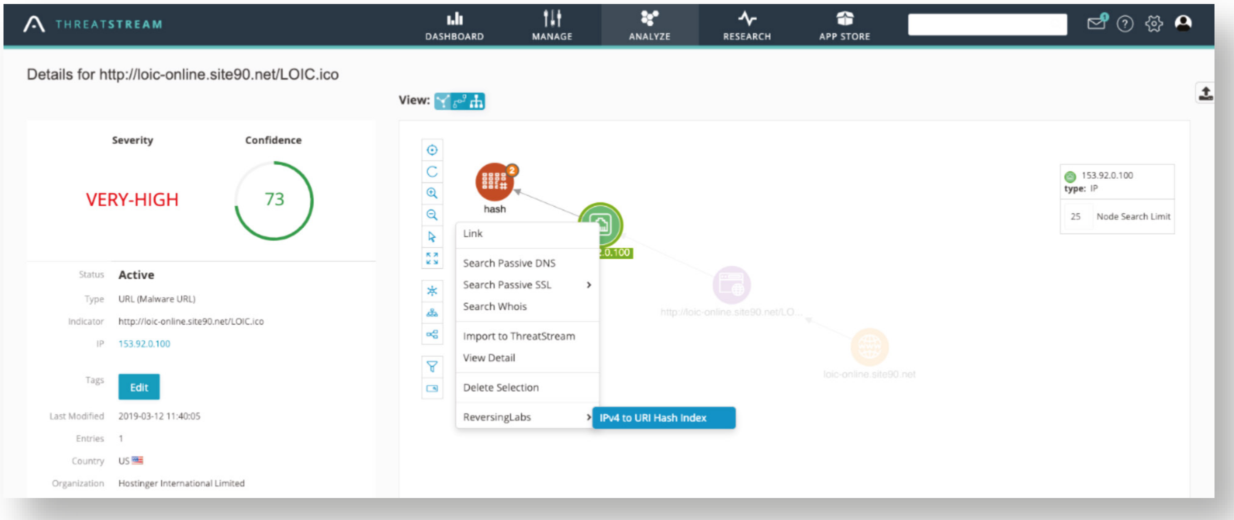
Details for b8670b2a25df70a1462428bd4290ed01980e0c18

Severity: VERY-HIGH
Confidence: 90

Status: Active
Type: Hash (Malware File Hash)
Indicator: b8670b2a25df70a1462428bd4290ed01980e0c18
Tags: Edit
Last Modified: 2019-04-18 08:45:42
Entries: 1
Insights: Antivirus detection ratio of 51/68 for file b8670b2a25df70a1462428bd4290ed01980e0c18 which was characterized as: Trojan.Win32.GenericKD

148949ad0123af4d87c7c7551f735285...
type: Hash
2e77d3ca122540debb758a25280e8fe9...
type: Hash
a399fe375f23aa31ac340a76c01374c0...
type: Hash
fbbe6b56e833dae6c8bc7cf832e0208a...
type: Hash
18a590df6b2c56db7b2dff988ba499db...
type: Hash
b96ab9dd6a17a4a5d8f3eb1d582c4450...
type: Hash
b1550efca74674a25dfde429ce9d9e66...
type: Hash
1e2589c234cf0cdc7be46ab603e5fa41...
type: Hash

4. **Display 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.



Details for http://loic-online.site90.net/LOIC.ico

Severity: VERY-HIGH
Confidence: 73

Status: Active
Type: URL (Malware URL)
Indicator: http://loic-online.site90.net/LOIC.ico
IP: 153.92.0.100
Tags: Edit
Last Modified: 2019-03-12 11:40:05
Entries: 1
Country: US
Organization: Hostinger International Limited

How It Works

- ReversingLabs offers API's for file-based malware threat intelligence, and premium feeds with the latest global detection results directly to Anomali ThreatStream.
- Evaluate and purchase from the Anomali APP Store:
  - Login to the Anomali Threat Platform,
  - Go to the Anomali APP Store and request a trial version of ReversingLabs APIs and Feeds to try it out for yourself.

ReversingLabs Solution Components

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

1. **File Reputation** - TCA-0101. File reputation from the authoritative cloud source, 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 AV detections. This is your go-to tool for file-based threats, allowing rapid identification and detection.
2. **AV Detections** - TCA-0103. The most recent cloud AV scan results with vendor, threat name, scan date provides useful pivoting data for actionable correlation and investigation intelligence.
3. **Enrichment** of RHA Functional Similarity - TCA-0301. Pivot from SHA-1 hash to functionally-similar malware within known malware families.
4. **Enrichment of URL to File Hashes** - TCA-0401. From a Domain, IP Address, Email Address or URL Find hashes of malware associated with the source Show summary reputation for each associated hash.

❷ 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 (Additional feeds are scheduled for integration during 2019):

1. **New Exploit/CVE Samples** (TCF-0203)
2. **New Linux Malware** (TCF-0104)
3. **New MacOS Malware** (TCF-0103)
4. **New Android Malware** (TCF-0102)

❸ Hash Links to the A1000 Advanced Malware Analysis Platform for further malware investigation.

About ReversingLabs

Malware routinely evades detection and lurks within corporate infrastructures causing damage and loss. Unique automated static analysis technology and authoritative file intelligence services power our innovative solutions that enable security teams to combat unknown malware. TitaniumScale high volume analysis and classification creates local threat intelligence across all internal objects, and empowers security teams to identify and neutralize malware that evades detection. For more information, visit us at www.reversinglabs.com

About Anomali

Anomali® detects adversaries and tells you who they are. Organizations rely on the Anomali Threat Platform to detect threats, understand adversaries, and respond effectively. Anomali arms security teams with machine learning optimized threat intelligence and identifies hidden threats targeting their environments. The platform enables organizations to collaborate and share threat information among trusted communities and is the most widely adopted platform for ISACs and leading enterprises worldwide. For more information, visit us at www.anomali.com