ANOMALI

REVERSINGLABS

Resilience starts here.

Detect and respond ... with Anomali and ReversingLabs

ANOMALI AND REVERSINGLABS JOINT SOLUTION OVERVIEW

- Titanium Cloud APIs for Anomali ThreatStream Enrichment to investigate threats
- Titanium Platform Ransomware Feed provides high fidelity, actionable ransomware intelligence into the Anomali ThreatStream platform
- Titanium Platform ELMA Feed provides the latest malware
- Submit hashes to the A1000 Threat Analysis and Hunting Workbench for further investigation

IMMEDIATE TIME-TO-VALUE

- Enrich hashes with TiCloud's up-to-date file reputation services, with definitive threat classification and rich context on over 12 billion files, directly from your ThreatStream user interface.
- ReversingLabs Ransomware Intel Feed provides analysts with indicators harvested from active, confirmed malware which is strictly vetted and curated to eliminate false positives.
- ReversingLabs ELMA feed enables researchers and detection engineers to investigate and detect the latest Windows, MAC, Linux and Android malware.
- Seamless integration with A1000 allows users to continue their investigation in the A1000 malware appliance.

RANSOMWARE FOCUSED INTELLIGENCE

ReversingLabs Ransomware Feed indicators are harvested from the +2.5 million confirmed, unique malware files analyzed every day producing a wealth of ransomware-related datasets

ENRICHMENT FROM A SINGLE PANE OF GLASS

ReversingLabs Titanium Cloud API can be accessed directly from an indicator in your ThreatStream view to enrich file hash indicators

COMBAT ALERT FATIGUE

Indicators from the ReversingLabs Ransomware Intel Feed are strictly vetted and curated to ensure indicators are not only accurate but active within the last 30 days, eliminating false positives

INDICATOR ENRICHMENT IN A SINGLE VIEW

CHALLENGE

Attackers are constantly updating malware sometimes making only minor changes to evade detection. Many threat intel providers do not deliver a definitive decision about suspected malware leading to inconsistency in analysis and requiring the user to do additional analysis.

SOLUTION

The ReversingLabs Titanium Cloud API integration provides up-to-date file reputation services, threat classification and rich context on over 12 billion goodware and malware files directly from an indicator in your ThreatStream view. This provides analysts access to the largest file reputation repository in the industry, delivering definitive answers, AV insights as well as malware family enrichments with a single click directly from your analyst view.

CUSTOMER BENEFIT

Access to the largest file reputation repository in the industry enables analysts to make better and faster decisions without having to use multiple tools, thereby reducing triage escalations.

ACTIONABLE REAL-TIME MALWARE RECOGNITION

CHALLENGE

Intelligence feeds are often populated with outdated information or siloed views of malware due to the limited view that many providers have of malware being delivering to victims. In addition, the indicators often lack the context needed for analysts and researchers to take action.

SOLUTION

ReversingLabs Ransomware Intel Feed provides Threat Intelligence teams with actionable indicators harvested from confirmed active malware. On average, 2.5 million unique malware files are analyzed every day to produce a wealth of ransomware-related datasets that encompasses more than 12 billion classified files, 3 billion of them malicious. These indicators are strictly vetted and curated, ensuring indicators are of high quality with no false positives. Indicators are enriched with MITRE ATT&CK tags, network, and malware family names ensuring action can be taken when a match is identified.

Coupling this file intelligence with Anomali Match big data analytics provides a real-time ransomware recognition solution that generates alerts with precision and confidence. Additionally, the Anomali big data analytics engine can leverage the Ransomware Feed indicators to conduct aggressive retroactive hunting campaigns using the rich metadata tagging applied to our indicators.

CUSTOMER BENEFIT

Actionable Intelligence curated specifically for identifying ransomware injected into Anomali's big data analytics engine provides the ability to catch ransomware in real time.

info@anomali.com | www.anomali.com
808 Winslow St, Redwood City, CA 94063 USA
1-844-4-THREATS

ANOMALI