ANOMALI® REVERSINGLABS

CONTINUOUS INTELLIGENCE FEEDS

Authoritative threat intel and powerful pivot toolkits delivered automatically to ThreatStream

ANOMALI AND REVERSINGLABS JOINT SOLUTION FEATURES:

- ReversingLabs threat intelligence feeds, including new malware not yet detected in the wild, drives automated response across existing security investments and gives enterprises deep visibility into attacks instantly.
- Award winning Titanium Platform returns authoritative file intelligence for enrichment and hunting, including investigative pivots, in response to threat lookups from the Anomali ThreatStream console.
- Supports threat detection in ThreatStream by:
  - Providing threat feeds from Titanium Platform, the largest private repository of authoritative file and malware information
  - Instantly displaying exposed file reputation, threat name, severity, historic AV detection rates, and more
  - Uncovering identifiers for functionally-similar executables using ReversingLabs Hashing Algorithm (RHA)
  - Providing access to an index of malware related to URLs, IP addresses, email addresses and domains to detect lurking malicious code across networks and endpoints

IMMEDIATE TIME-TO-VALUE

- Accelerate incident response and threat mitigation by enriching alerts in ThreatStream and associated security controls with the latest, emerging malware threat details
- Malicious files identified and displayed in ThreatStream with file reputation, threat classification, severity, historic AV detection rates - to help threat hunting teams rapidly respond and update security controls
- Protects against complex attacks and hidden payloads from targeted and polymorphic malware by enriching ThreatStream with new intelligence sent to security controls for preventive security, with deep details for pivoting to expose malicious code across systems

AUTOMATE MALWARE DETECTION AND HUNTING

Malware routinely evades detection and lurks within corporate infrastructures causing damage and loss. Unique automated static analysis technology and authoritative file intelligence services power ReversingLabs innovative solutions that enable security teams to combat unknown malware. Titanium Platform 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.

CRITICAL INTELLIGENCE

Access to malware and goodware file classification, an index of URLs related to IP addresses, email addresses, domains to identify associated attacks

FLEXIBLE DEPLOYMENTS

Fast, scalable implementation on-premises and in the cloud

IMMEDIATE RESULTS

Pre-execution protection against emerging threats that are instantly identified using the continuously updated authoritative file analysis results from TitaniumCloud, the largest private file repository

CASE STUDY

CHALLENGE:

Faster incident response through actionable intelligence.

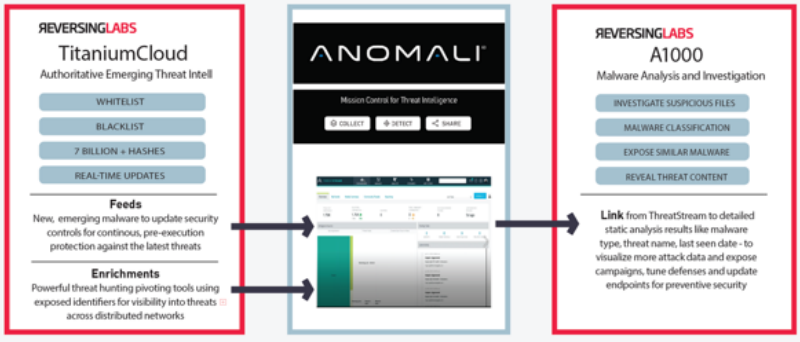
SOLUTION:

ReversingLabs Titanium Platform threat intelligence feeds, including file hashes of new malware, are integrated into Anomali ThreatStream and can be leveraged to update security controls for preventive security and automate containment of files pre-execution. The feeds are from ReversingLabs TitaniumCloud, the authoritative file intelligence repository which instantly serves up file hash, file type, and current A/V detections for rapid detection of hidden malware.

CUSTOMER BENEFIT:

The ReversingLabs threat feeds deliver comprehensive malware intelligence including insights to new, in-the-wild malware directly to ThreatStream and associated security controls for preventive security, ensuring customers are protected against latest.

ReversingLabs - Anomali ThreatStream Architecture Workflow



CASE STUDY

CHALLENGE:

Closing security gaps with insights into destructive objects.

SOLUTION:

ReversingLabs exposes powerful threat hunting pivoting tools in ThreatStream using data like threat name and severity, historic AV detection rates, and indexes of associated URLs, IP addresses, email addresses and domains. Investigative pivots and advanced search optimize threat hunting activities to detect malware and lurking malicious code. To further investigate alerts, drill-down capabilities are filtered and sorted in real-world language, for the most actionable data available.

CUSTOMER BENEFIT:

The ReversingLabs malware intelligence is displayed in ThreatStream with details about the file, threat name, when we first saw it, for example, to help threat hunting across networks and endpoints for associated lurking malware and related threats. For example, an attack campaign can be exposed by pivoting on the new threat intel to gather more data about the hash to develop and expand analysts view into the attack and where else it may be lurking by adding a few more hashes and pivoting for similarity on them.

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

ANOMALI®