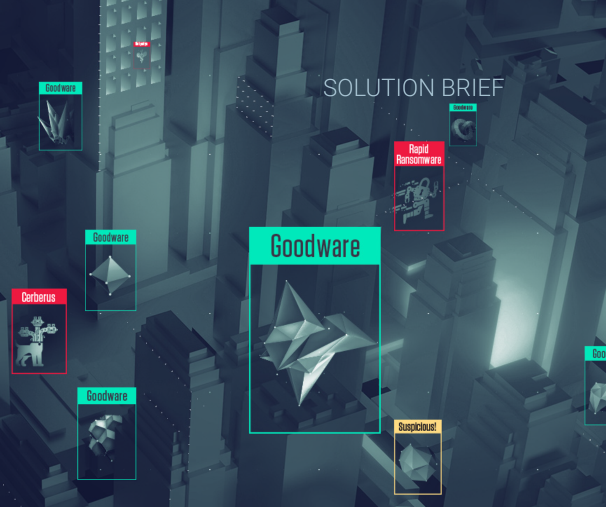
REVERSINGLABS

SOLUTION BRIEF



ReversingLabs Titanium Platform

Delivers explainable threat intelligence into every destructive file and object to help Security Operations Center (SOC) and Software Development teams detect, identify, and respond to the latest attacks and risks associated with third-party software.

Key Differentiators

- **SPEED FILE ANALYSIS WITH ACTIONABLE INTELLIGENCE**
  Speed detection of files and objects through automated static analysis, prioritizing the highest risk files with actionable details, in only milliseconds.

- **ACCURATE THREAT DETECTION**
  Accurately detect threats with the largest repository of 12 billion malware and goodware files and over 4000 formats, while maintaining privacy.

- **SEAMLESSLY INTEGRATE AT SCALE**
  Enterprise customers process billions of objects per week while integrating insights across the entire enterprise.

- **DEEP INVESTIGATION**
  Deep investigation of malware infected files for threat hunters and incident responders through advanced search, custom YARA rules and retro-hunt.

> “The Malware and Threat Intelligence teams love it. I hear feedback from them all day about products that don't meet expectations, but ReversingLabs is never mentioned on that list! I can’t wait to find out how we can leverage ReversingLabs in more ways across our SOC. I've had a really great experience dealing with ReversingLabs, especially with support.

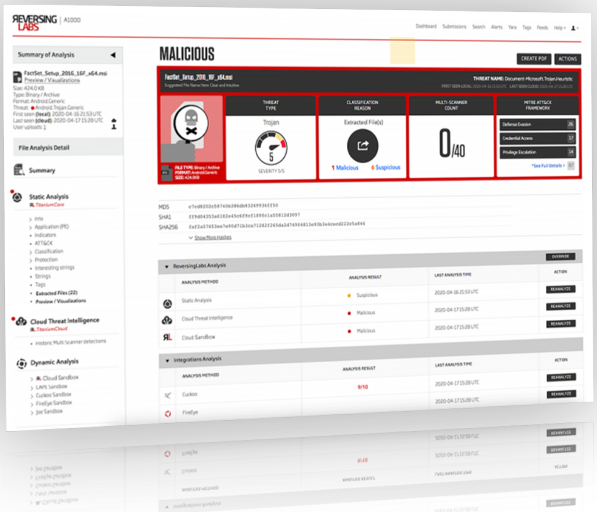
Insurance Company,
Enterprise Architect

Business Challenge

Organizations advancing their business through new digital strategies continue to take on brand, financial and information risks due to the growth of malware infected files and objects sourced from the web, email, supply chain, cloud, mobile, and APIs. These advanced and destructive objects are armed to circumvent existing anti-virus, EDR, email protection, sandbox and threat intelligence solutions leaving companies blind to threats lurking within their network. This is having an impact on the CISO’s ability to achieve top security and business initiatives. Whether it’s clearer security metrics focused on high risk threat vectors such as phishing, automating security and SOC operational processes to help fill the security skills gap, enabling the secure migration of apps to more modern architectures, or the acceleration of secure app development to compete in today’s digital economy, malware infected objects are the primary issue in mitigating today’s attacks.

Solution

ReversingLabs solves the problem preventing those from meeting security objectives, through the delivery of advanced malware analysis and insights into destructive files and objects. The automated static analysis and file reputation platform, delivers the fastest and most accurate malware insights in the industry. The Titanium Platform is delivered as a hybrid cloud delivery model providing connectors that integrate with EDR, Network Security, Email, SIEM, TIP, and Sandboxes. The platform reduces incident response time for SOC analysts, while providing detailed threat information for hunters to take quick action. ReversingLabs delivers the explainable threat intelligence needed to help SOCs confidently verify alerts, automate incident response and develop threat skills one event at a time.



Size: 424.0 KB
Type: Binary / Archive
Format: Android.Generic
Threat: Android.Trojan.Generic
First seen (local): 2020-04-16 21:53 UTC
Last seen (cloud): 2020-04-17 15:28 UTC
User uploads: 1

THREAT NAME: Document-Microsoft.Trojan.Heuristic

FILE TYPE: Binary / Archive
FORMAT: Android.Generic
SIZE: 424.0KB

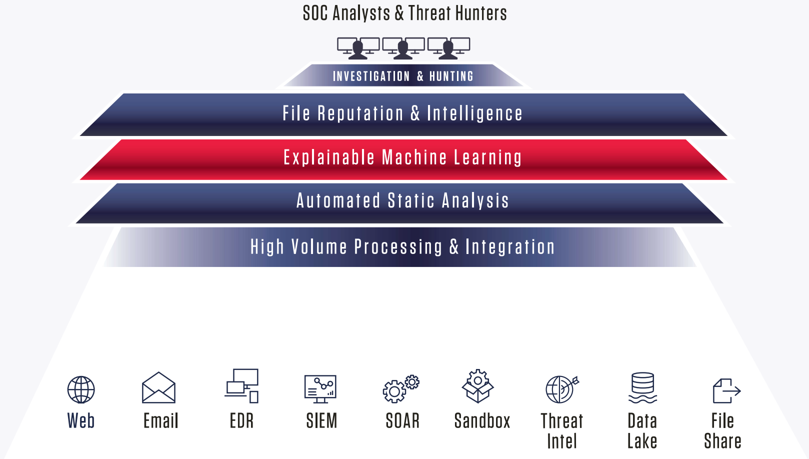
ReversingLabs Analysis

ANALYSIS METHOD	ANALYSIS RESULT	LAST ANALYSIS TIME	ACTION
Static Analysis	Suspicious	2020-04-16 21:53 UTC	REANALYZE
Cloud Threat Intelligence	Malicious	2020-04-17 15:28 UTC	REANALYZE
Cloud Sandbox	Malicious	2020-04-17 15:28 UTC	REANALYZE

Integrations Analysis

ANALYSIS METHOD	ANALYSIS RESULT	LAST ANALYSIS TIME	ACTION
Cuckoo	9/10	2020-04-17 15:28 UTC	REANALYZE
FireEye		2020-04-17 15:28 UTC	REANALYZE

TITANIUM PLATFORM


SOC Analysts & Threat Hunters
INVESTIGATION & HUNTING
File Reputation & Intelligence
Explainable Machine Learning
Automated Static Analysis
High Volume Processing & Integration
Web
Email
EDR
SIEM
SOAR
Sandbox
Threat Intel
Data Lake
File Share

Titanium Platform Capabilities

Automated Static Analysis [TitaniumCore]

- ***Formats:*** 4000 file formats with over 400 file formats unpacked and analyzed including archives, installers, packers & compressors.
- ***Decomposition:*** Automated Static Analysis decomposes files without execution within milliseconds.
- ***Indicators:*** Threat indicators generated for every sample and extracted from all objects.
- ***Classification:*** 5 levels of classification including known, unknown, suspicious, malicious and good.
- ***Compared:*** Functional similarity to known malware using ReversingLabs Hashing Algorithm.

Explainable Machine Learning (ML)

- ***Human-Readable Indicators:*** Generates human readable descriptions across 12,000+ file indicators within malware code and metadata properties.
- ***Verifiable Classification:*** Provides visual tags to explain which indicators have contributed to final classification verdicts, thus supplying the "how" a decision was made.
- ***Full Transparency:*** Exposes the logic and most significant contributions behind each classification, and why each of these indicators had been triggered.
- ***MITRE ATT&CK Support:*** Links indicators to respective MITRE ATT&CK framework categories, helping SOC analysts understand the type of threat they are dealing with and its impact to the organization.

File Reputation [TitaniumCloud]

- ***Goodware/Malware:*** 12 billion files stored for goodware and malware search queries, with 8 million updates daily for the most up-to-date file reputation status.
- ***AV:*** Historical detection results from 40+ AV Vendors yields industry reputation consensus while showing changes over time.
- ***Dynamic Analysis:*** Submit high severity files for detonation in ReversingLabs cloud sandbox for additional insights to malware behavior.
- ***Files:*** Over 400 packed file formats processed and 4000 file formats identified from diverse platforms, applications and malware families.
- ***Privacy:*** Single source of global file reputation data - private, not publicly crowd-sourced.

High Volume Processing & Integration [TitaniumScale]

- ***Runtime:*** Real-time, deep inspection of files from web traffic, email, file transfers, endpoints or storage, while scaling to 100 million files per day without dynamic execution.
- ***APIs:*** 50+ APIs and feeds automate processing, analysis and threat status information gathering.
- ***Connectors:*** Tightly coupled connectors seamlessly integrate industry leading email, EDR, Network Security, SIEM, SOAR, and analytics platforms.

Investigation [A1000]

- ***Persona UI:*** Threat intelligence, analysis and hunting teams use as a primary workbench for deep file analysis, accelerating investigations and response activities.
- ***Search & Hunt:*** 500+ search expressions with support for boolean operators and auto-completion.
- ***YARA Rules:*** ReversingLabs or customer supplied YARA rules classify files by advanced rules engine, with support of up to 250 rules per ruleset for retro-hunting.

Optimize Existing Security Investments

Email

Find high priority threats missed by email gateways and abuse boxes.

EDR

Enrich malware detection with detailed malware threat information.

AppSec

Inspect release images for thirdparty software risks including malware, compromised certificates, etc.

Anti-Virus

Detect files without signatures, with a size and complexity not addressed by AV.

Threat Intel

Complement external threat intelligence platforms with local file and object visibility.

Integration

Unify and seamlessly integrate into existing security investments with malware insights.

Sandbox

Optimize sandbox file processing with only the highest priority malware while avoiding evasive techniques.

SIEM & SOAR

Reduce MTTR and automate response with high priority good/bad malware classification.

REVERSINGLABS
Worldwide Sales : +1.617.250.7518
sales@reversinglabs.com