REVERSINGLABS

Recorded Future

Intelligence Cards Enriched with Rich Threat Hunting Data

Accelerates Malware Hunting, Correlation and Response with a Comprehensive, Integrated Solution

ReversingLabs TitaniumCloud industry-leading file reputation data is integrated with Recorded Future's Intelligence Cards core platform to accelerate an organization's ability to identify suspicious files, respond to threats and update security devices against future malware attacks.

Premium ReversingLabs TitaniumCloud APIs and integration with our A1000 Malware Analysis Platform can be turned on in the Recorded Future Complete Privilege Extended Intel Cards with an upgrade.

Recorded Future's contextualized threat intelligence is a key component of a proactive security strategy. Recorded Future Intelligence Cards can be enriched using ReversingLabs TitaniumCloud file intelligence to provide extended metadata on files, malware, and IP addresses and domains. With these extended Intelligence Cards, organizations have instant access to the most up-to-date and relevant malware information available, a critical weapon in the fight against skilled attackers who rapidly morph their techniques to hide their intent and actions. ReversingLabs integrates its premium TitaniumCloud API's with Recorded Future via extensions built into Hash, Malware and IP/Domain Intelligence Cards that can be turned on to enrich these cards with more detailed TitaniumCloud results and A1000 malware analysis platforms results. These enriched Extended Intelligence Cards allows security operations center (SOC) teams and threat intelligence analysts to access the deep analysis results from a single, integrated report to gain insight into critical, file-based threat information.

From these Extended Intelligence Cards, SOC teams can pivot on key metadata such as file hashes, malware family and threat actor names within the Recorded Future platform. The result is a more efficient and effective process for fully investigating suspicious files in order to rapidly respond, remediate, and update security defenses.

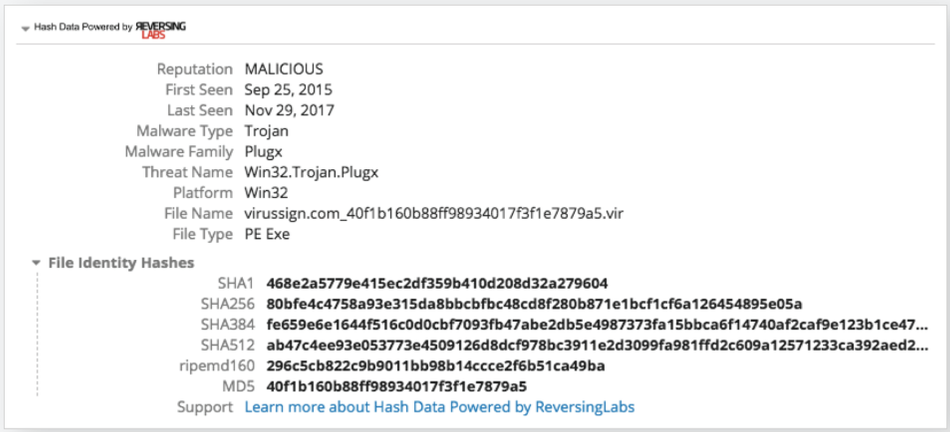
Solution Highlights

- **All Recorded Future customers have access to basic file reputation information on Hash Intelligence Cards for correlated file intelligence and threat intelligence to detect even the most sophisticated advanced malware.**

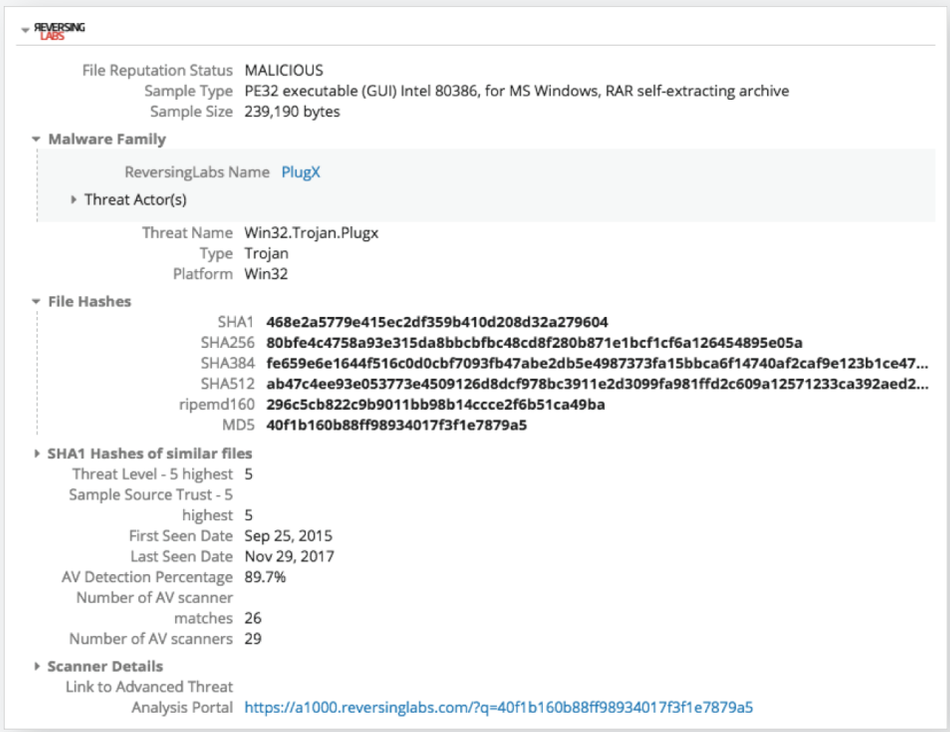
- **Recorded Future customers can subscribe for additional file intelligence to visualize more attack data in Hash, Malware and IP/Domain Extended Intelligence Cards from ReversingLabs - such as data on specific hashes and malware families, to find malware and tune defenses.**

- **Pivot on specific and reliable ReversingLabs file intelligence results on malware, threat actors and more within the Recorded Future platform using Extended Intelligence Cards.**

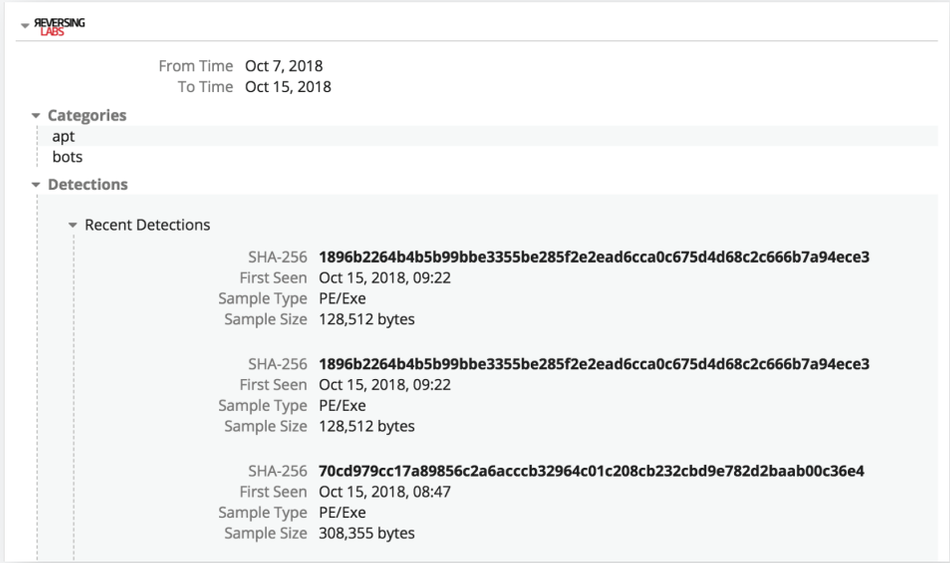
- **Analyze and visualize suspicious files in detail - with just one click - using the ReversingLabs A1000 Malware Analysis Platform.**



Hash Intelligence Card basic results for all RF customers **OUT OF THE BOX**

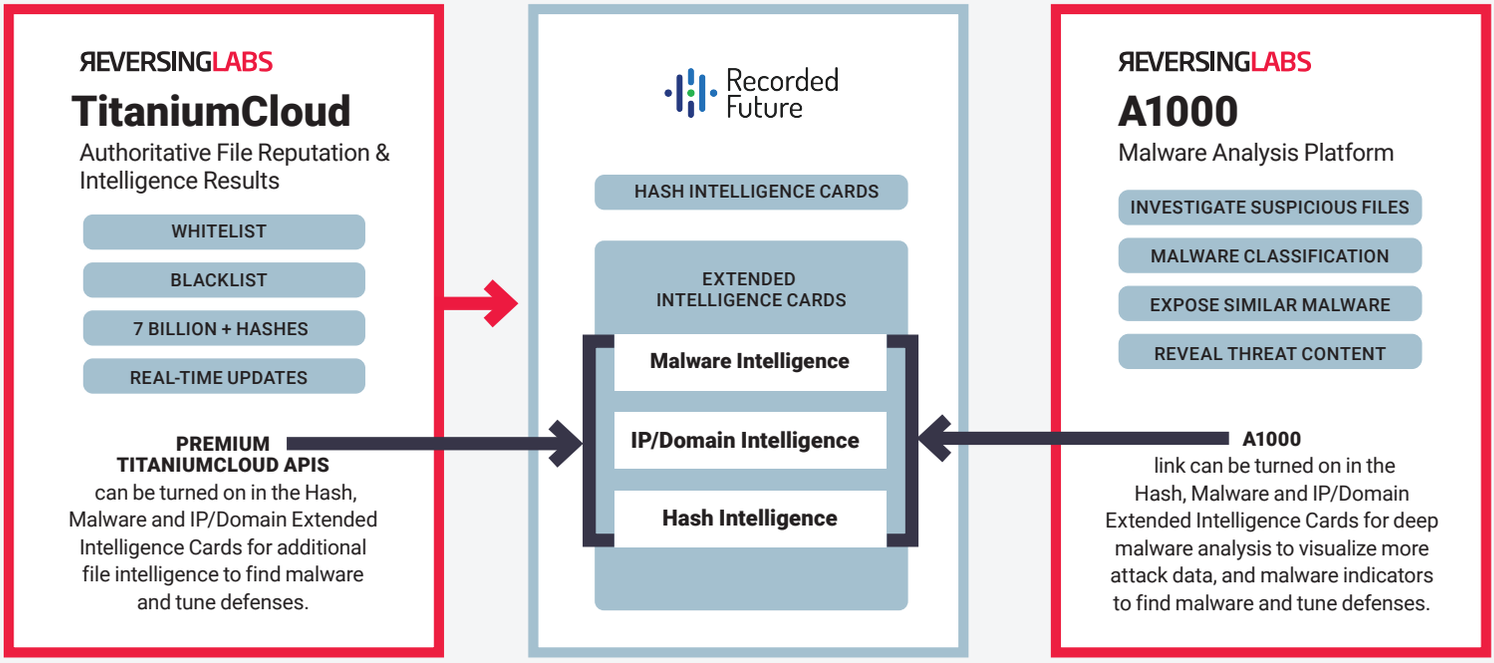


Hash Intelligence Card results with **LIMITED PRIVILEGE** credentials



Hash Intelligence Card results with **COMPLETE PRIVILEGE** credentials

ReversingLabs - Recorded Future Architectural Workflow



ReversingLabs commercial extension requires licenses for the following APIs & feeds for Limited and Complete Privileges:

LIMITED PRIVILEGES

TCA-0101 File reputation (Malware Presence)
TCA-0103 Historic Scan Records (Xref)
TCA-0301 RHA Functional Similarity
TCA-0401 URI to Hash Search (List of file hashes associated with given URI)

COMPLETE PRIVILEGES

TCA-0101 File reputation (Malware Presence)
TCA-0103 Historic Scan Records (Xref)
TCA-0301 RHA Functional Similarity
TCA-0304 Malware Family Search (Return List of Hashes based on input string)
TCA-0312 APT Indicator Search (Returns new malware hashes belonging to APT tool or actor)
TCA-0313 Financial Services Indicator Search
TCA-0314 Retail Sector Indicator Search
TCA-0315 Ransomware Search
TCA-0316 CVE Search
TCA-0401 URI to Hash Search (List of file hashes associated with given URI)

How It Works

ReversingLabs file reputation and automated static analysis integrates with Recorded Future's Intelligence Cards so organizations have all the data they need in one place to fully investigate suspicious files for enhanced response, remediation, and future preparedness.

- As a standard feature, ReversingLabs' file reputation and automated static analysis access is built into Recorded Future Hash Intelligence Cards and is accessible at the top of the card indicated as "Hash Data Powered by ReversingLabs." Hash Intelligence Cards display basic file reputation information powered by ReversingLabs, enriching Recorded Future collected data with authoritative file reputation data from the authoritative global file reputation database of 7 billion known goodware and malware files.
- With a paid subscription to TitaniumCloud, Recorded Future Extended Intelligence Cards are enriched with specific metadata such as file hashes, malware families, APT indicators and much more. Extended File Intelligence Cards for Hash, Malware and IP/Domain Intelligence Cards also include 1 click pivoting on File Hashes, Malware Family Name and Threat Actor Names within the Recorded Future platform. Extended Intelligence Cards also include a link to ReversingLabs A1000 Threat Analysis platform to perform further analysis such as file download, rescans, functional similarity analysis and YARA rule generation.
- With the detailed file analysis, visualization and advanced hunting from the ReversingLabs platform enriching Intelligence Card data, the solution connects organizations' threat intelligence, file intelligence, and file analysis together into an integrated solution so security analysts, threat hunters and forensic investigators have the data and context they need to find, investigate, identify and respond to even the most sophisticated advanced malware.