A1000 Malware Analysis Platform

Hunt, Identify, and Analyze Advanced Malware

A1000 Features

- **Definitive File Analysis:** unpack, deobfuscate, extract internal indicators and assign threat levels in milliseconds.
- **Extensive Format Coverage:** includes PE, ELF, MachO, Dex, .NET, Java, JS, documents, firmware, and business apps.
- **Rich Context Visualizations:** view context, intent and severity for further action.
- **Integrated YARA Rules Engine:** utilize custom rules to identify/enable new and advanced malware detection.
- **Private File Analysis:** files are not shared publicly so files and results never leave your site.
- **Centralized Content Repository:** securely store files of interest for collaborative search, analysis, and hunting.
- **Automated Workflow Integration:** powerful REST APIs integrate with existing workflows and processes.

The A1000 Malware Analysis Platform supports advanced hunting and investigations through high-speed automated static analysis. It is integrated with file reputation services to provide in-depth rich context and threat classification on over 8 billion files including all file types. The A1000 supports visualization, APIs for integration with automated workflows, a dedicated database for malware search, global and local YARA rules matching, alert subscription and management, as well as integration with third-party sandbox tools.

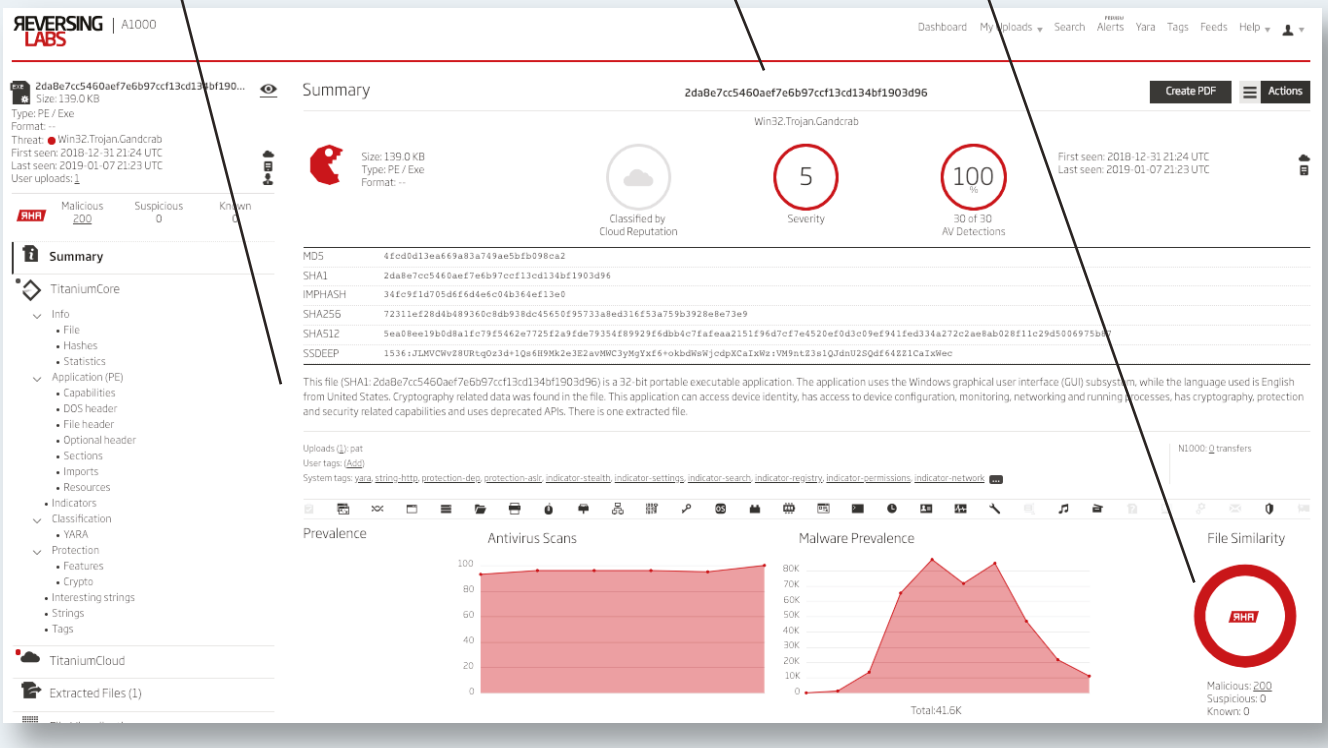
Visualizing Malware

The example below shows a file examined by the A1000 and highlights key areas of interest for analysts.

Provides summary of critical details and actions the malware may take or what is found, e.G. Has cryptography

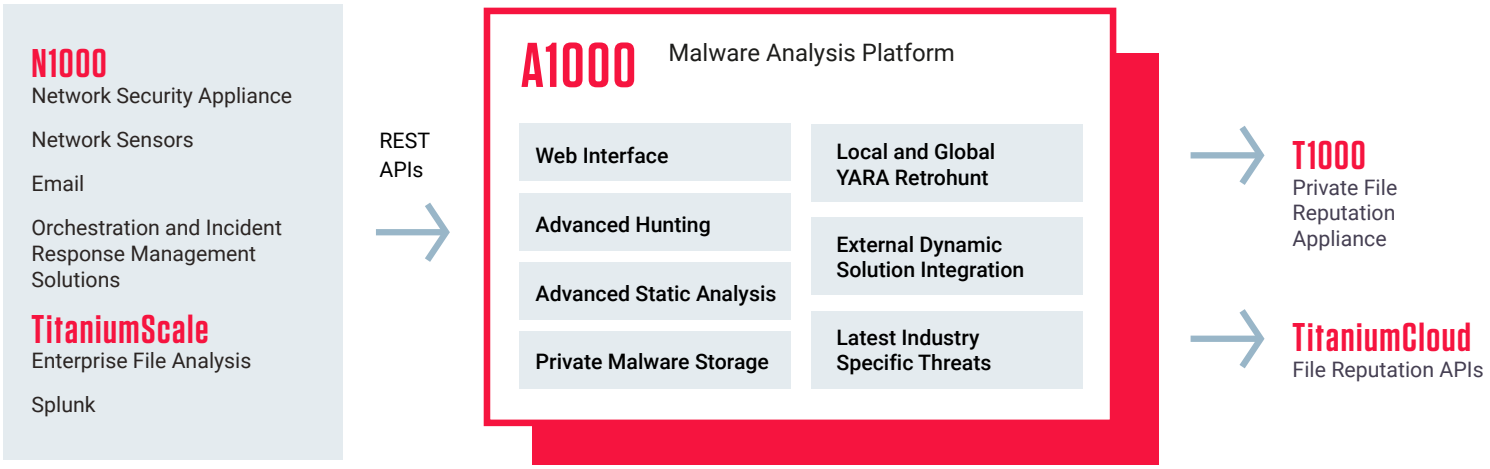
Integrated report that lists historical and other critical info that security analysts need

Lists functionally similar variants Classified by their detection and enables pivot on malicious samples



A1000 Malware Hunting and Analysis

The A1000 is the primary workbench for deep file analysis, accelerating investigations and response activities for threat intelligence, analysis and hunting teams. It assesses malware and malware status changes as malware families morph over time via obfuscation and other techniques. Integration with TitaniumCloud enables users to search across 8 billion goodware and malware files and to privately upload file samples for analysis.



A1000 Features

Integrated Malware Analysis & Investigation

- Analysis engine performs high-speed, static analysis to unpack files, extract internal indicators and assign threat levels.
- Integrated database enables safe, secure storage of results and enables sample search by threat indicators.
- Visualization GUI for quickly understanding critical info.

Automated Static File Analysis

- Processes files within milliseconds.
- Evaluates functional similarity to known malware.
- Builds and deploys custom YARA rules.
- Unpacks over 360 file formats of archives, installers, packers & compressors.
- Identifies more than 3600 file formats.
- Extracts over 3000 threat indicators.

Private Content Repository

- Provides safe storage of malicious/suspicious files.
- Stores file context in an onboard searchable database.
- Enables private, safe sample sharing / historical analysis.

Alerting Subscription and Management

- Subscribe up to 6 alerts with email notification.

Extensive Search & Advanced Hunting

- Search by hash, imphash, file name, #tags and more.
- Find and download files based on functional similarity.
- Supports user-defined YARA rules for matching and hunting.

Integrated with TitaniumCloud File Reputation Service

- Access to comprehensive, curated source of threat intelligence and reputation data on 8 billion goodware and malware for global context.
- Enables upload/download samples via GUI.
- Supports YARA rules search.

Advanced Hunting Options

- Advanced Search.
- Active-YARA and Retro-YARA.

Supports Integration

- Supports automated analysis workflows via REST Web services API.
- Integrates directly with Cuckoo and Joe Sandbox.

Delivered as

- Hardware, VMDK or cloud-based appliance.

REVERSINGLABS
Worldwide Sales : +1.617.250.7518
sales@reversinglabs.com