# A1000 Advanced Hunting Options

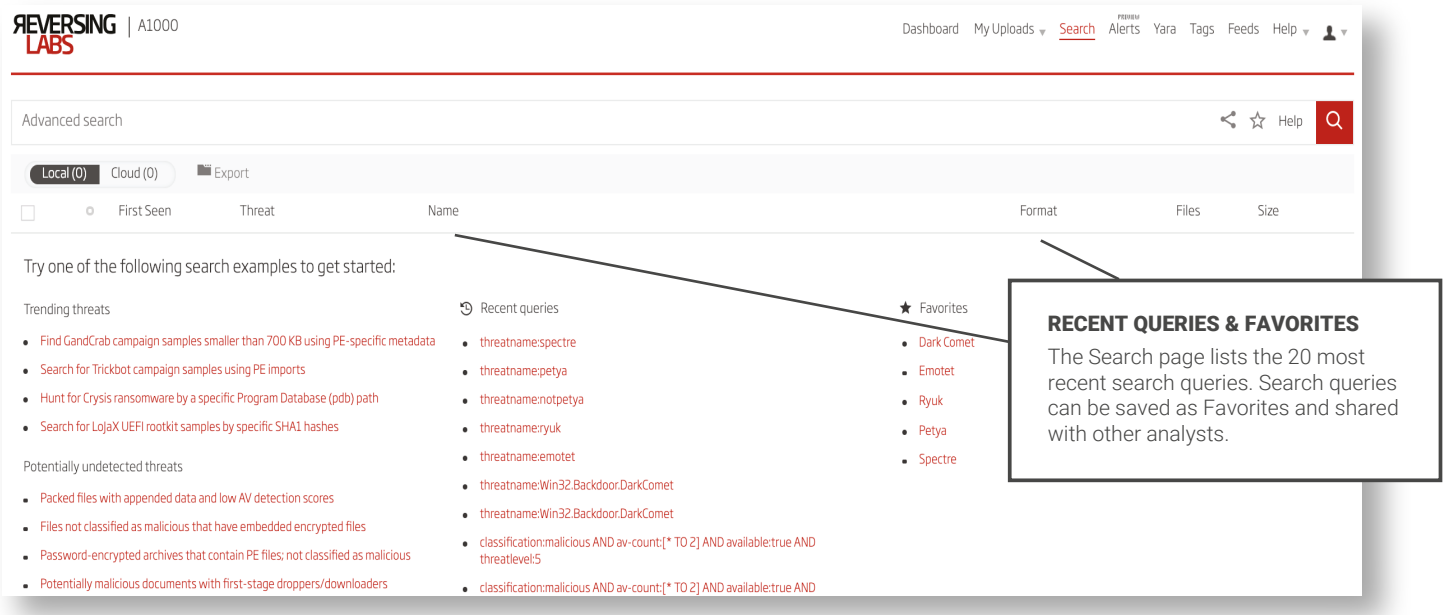
Powerful Search and YARA Features to Hunt Advanced Malware

## Key Features

- **Support for 500+ Search Expressions:** Supports more than 78 keywords, 32 anti-virus vendors, 137 sample types and subtypes and 283 tags enable building of 510 unique search expressions with support for Boolean operators and auto-completion.
- **Fast Results:** Typically less than 3 seconds for initial results with targeted search results within 24 hours.
- **Quick Hits and Pivoting Support:** Quickly and easily search and pivot on data for trending threats, emerging malware, network-related data, and document and certificate misuse.
- **YARA Ruleset Retrohunting:** Support of up to 250 rules per ruleset for a retrohunt and up to 10,000 each of cloud detections and local detections.
- **Retrohunt Visibility to 90 days:** Real-time updates and full results in less than 2 hours.
- **Retrohunt Manageability:** Full control to start and stop retrohunt jobs with progress reports via APIs or visualized on the A1000 to see real-time statistics.
- **Alert Subscription and Management:** Supports Alerts creation from multiple screens and workflows and provides alert notices upon resolution.

Building on the industry-leading A1000 Malware Analysis Platform, the A1000 with Advanced Hunting Options offers a range of sophisticated features to optimize search, YARA retrohunting and automate malware detection and alert notification. The advanced options of the A1000 makes searching of large data sets locally and in ReversingLabs' TitaniumCloud far easier, enables more powerful searches, increases coverage of the search, takes less time for each search and ultimately provides unprecedented visibility into historical data to uncover malware.

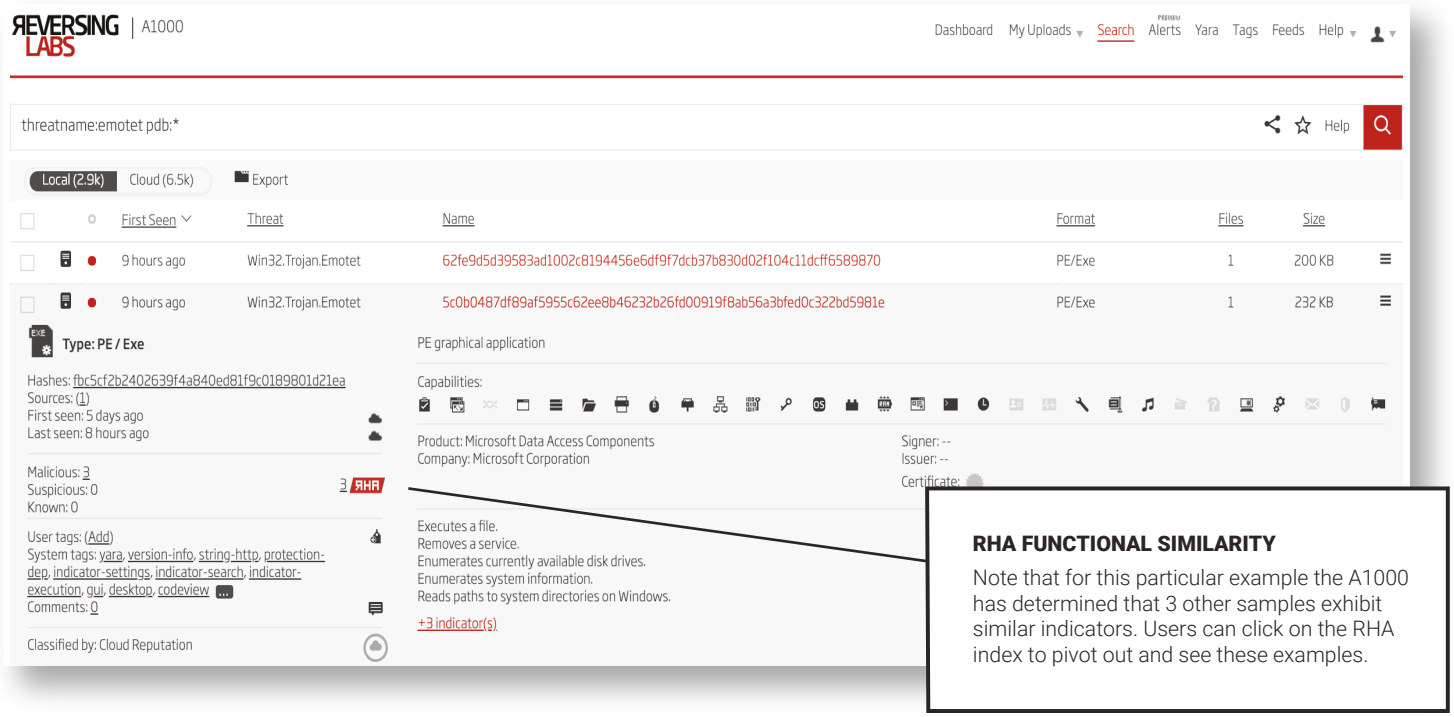
The A1000 with Advanced Hunting Options is a unified platform for sophisticated hunting and triage. Multi-conditional queries using logical expressions enable more efficient and effective searching. It enables analysts to use multiple YARA rulesets to traverse large historical sample sets quickly in order to greatly enhance detection and reduce impact from breaches and targeted campaigns. Analysts can subsequently be alerted for a variety of conditions, e.g. when a sample has changed detection levels, or when YARA rules have triggered, or when dynamic analysis has been completed.




Analysts can quickly start their investigations at the advanced search screen which offers one-click examples of trending threats, emerging malware, network related data, and documents and certificate misuse. The Search start page now lists 20 most recent search queries performed on the appliance. Users can save their search queries on A1000 as Favorites. Up to 20 Favorites can be created, and they will be listed on the Search start page next to the recent queries.

# Malware Intelligence with a Single Click

As shown below, analysts can quickly access a comprehensive set of file intelligence data by clicking on the samples. Both standard and advanced A1000 versions assess malware and malware status changes as malware families morph over time via obfuscation and other techniques.

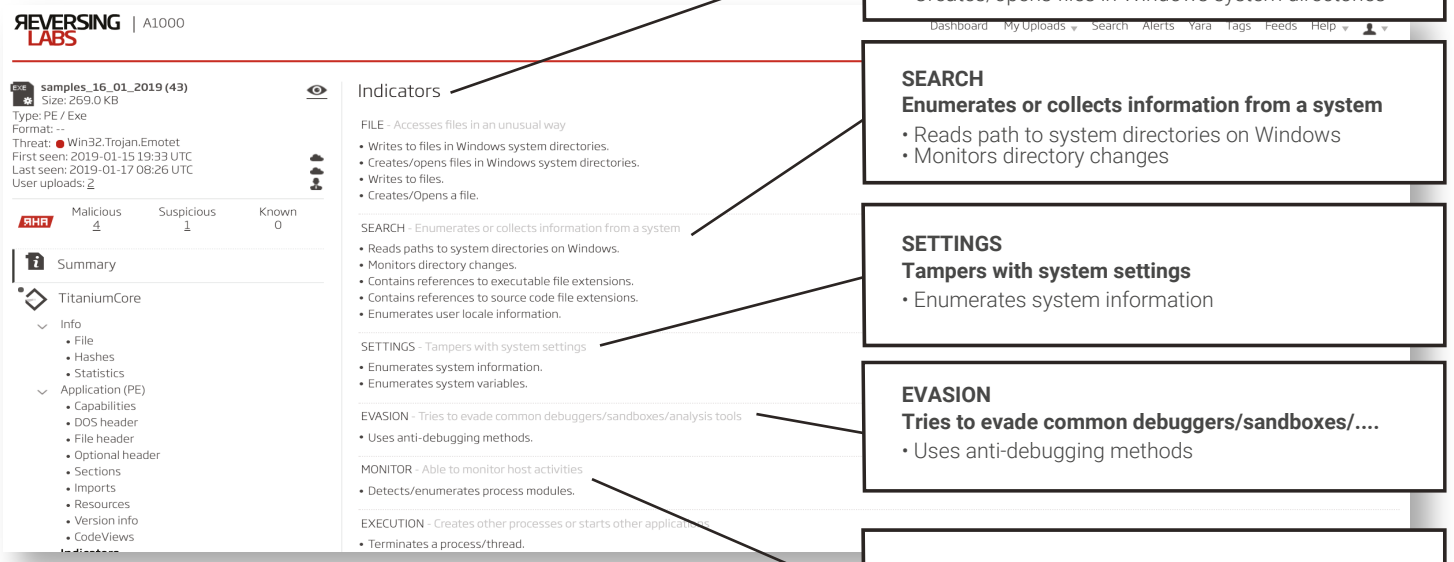



**RHA FUNCTIONAL SIMILARITY**

Note that for this particular example the A1000 has determined that 3 other samples exhibit similar indicators. Users can click on the RHA index to pivot out and see these examples.

# Threat Indicators

The Indicators screen shown below organizes information into categories such as Search, Settings, Evasion, Executions and other areas to point out if the malware is attempting such actions as; collecting system information, tampering with system settings, trying to evade common sandboxes or attempting to create other processes or start other applications.




**FILES**
**Accesses files in an unusual way**
- Writes to files in Windows system directories
- Creates/opens files in Windows system directories

**SEARCH**
**Enumerates or collects information from a system**
- Reads path to system directories on Windows
- Monitors directory changes

**SETTINGS**
**Tampers with system settings**
- Enumerates system information

**EVASION**
**Tries to evade common debuggers/sandboxes/....**
- Uses anti-debugging methods

**MONITOR**
**Able to monitor host activities**
- Detects/enumerates process modules

Threat intelligence, analysis and hunting teams utilize the A1000 as the workbench for deep file analysis to accelerate investigations and response activities. Integration with TitaniumCloud enables a more robust solution which allows users to search across 8 billion goodware and malware files and to privately upload file samples for advanced search analysis.

# A1000 Features

## MALWARE ANALYSIS PLATFORM

### Integrated Malware Analysis and 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 to enable sample search by threat indicators.
- Users can access data locally or in the cloud.
- 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.
- Identifies more than 3600 file formats.
- Unpacks over 360 file formats of archives, installers, packers and compressors.
- 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 and historical analysis.

### Search & 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.

## ADVANCED HUNTING OPTIONS

### Customer Option: Advanced Search

- Build powerful queries with search modifiers and operators.
- Select from hundreds of expressions and dozens of keywords.
- Leverage the autocomplete functionality for faster research.
- Identify files according to antivirus detections.
- Perform targeted queries on large sample datasets.
- Share and export search results on A1000 for further analysis.
- Up to 20 Search Favorites can be created, edited, and shared.

### Customer Option: Active YARA & Retro-YARA Rules

- Users can hunt through 90 days of data history.
- Real-time updates are provided with full results in < 2hrs.
- An ample amount of 250 rules per ruleset is available.
- A maximum of 10K Cloud + 10K Local Detections.
- Users can Start/Stop Retrohunts at anytime.
- Progress is reported via API or GUI for real-time updates.

### Alerting Subscription and Management

- Alerts subscribed to from multiple pages for speed and ease.
- Easy to subscribe to the following alerts:
    1. Classification change
    2. Sample availability
    3. YARA Ruleset match
    4. Cuckoo Analysis complete
    5. File Upload complete
    6. TitaniumCloud AV scan complete.
- Alerts communicated via email.
- Sort and Filter Alerts.
- Alert notices upon resolution.



REVERSINGLABS

**Worldwide Sales : +1.617.250.7518**
**sales@reversinglabs.com**