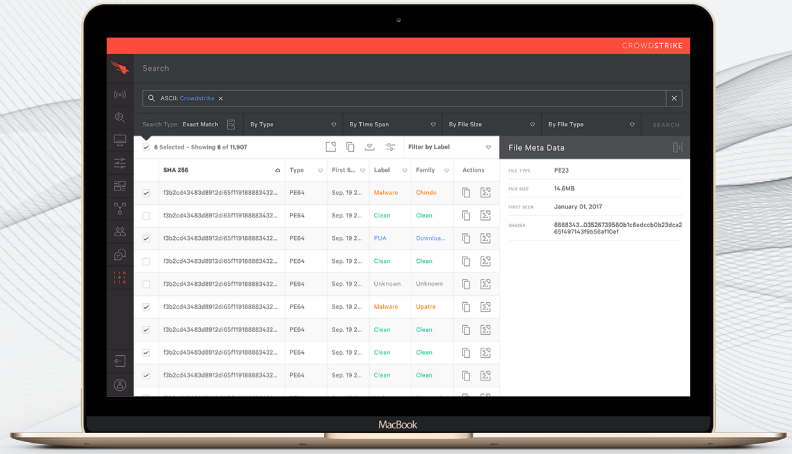
CROWDSTRIKE

FALCON MALQUERY

Fast, comprehensive malware search

CrowdStrike has amassed an ever-expanding, comprehensive real-time repository of threat events and artifacts stretching back years. With the CrowdStrike Falcon Search Engine, this treasure trove of threat data is put at the disposal of security professionals and helps them better protect their organizations.

CrowdStrike's Falcon MalQuery is an advanced, cloud-based malware research tool that enables security professionals and researchers to quickly search a massive dataset of malware samples, validating potential risks and staying ahead of would-be attackers. At the core of Falcon MalQuery, is a large, multi-year collection of malware samples, indexed by patent-pending technology resulting in rapid search.



ASCII: Crowdstrike ×

Search Type: Exact Match

☑ 6 Selected – Showing 8 of 11,907

	SHA 256	Type	First S...	Label	Family	Actions
☑	f3b2cd43483d8912di65f119188883432...	PE64	Sep. 19 2...	Malware	Chindo	
□	f3b2cd43483d8912di65f119188883432...	PE64	Sep. 19 2...	Clean	Clean	
☑	f3b2cd43483d8912di65f119188883432...	PE64	Sep. 19 2...	PUA	Downloa...	
□	f3b2cd43483d8912di65f119188883432...	PE64	Sep. 19 2...	Clean	Clean	
□	f3b2cd43483d8912di65f119188883432...	PE64	Sep. 19 2...	Unknown	Unknown	
☑	f3b2cd43483d8912di65f119188883432...	PE64	Sep. 19 2...	Malware	Upatre	
☑	f3b2cd43483d8912di65f119188883432...	PE64	Sep. 19 2...	Clean	Clean	
☑	f3b2cd43483d8912di65f119188883432...	PE64	Sep. 19 2...	Clean	Clean	
☑	f3b2cd43483d8912di65f119188883432...	PE64	Sep. 19 2...	Clean	Clean	

File Meta Data

FILE TYPE	PE23
FILE SIZE	14.6MB
FIRST SEEN	January 01, 2017
SHA256	8888343...03526739560b1c6edccb0b23dca265f497143f9b56af10ef

MALWARE SEARCH AT THE SPEED OF THE CLOUD

Falcon MalQuery establishes a new standard for quick, easy and comprehensive malware search for security professionals who need to determine the validity of a threat and take action to stop it.

KEY BENEFITS

- Fast: Get results in seconds, not hours, for quicker threat response
- Comprehensive: Search a massive, continuously-updated threat dataset
- Precise: Reduce false positives by creating high-precision YARA rules
- Alerting: Persistent searches alert you when a new malicious sample appears
- Simple search: Input simple strings
- YARA search: Flexibility to accept YARA rules instead of simple search terms

MalQuery is the major step forward in malware research that security professionals have been asking for, enabling them to move faster than the adversary and gain the tactical advantage needed to defend their organization against today's sophisticated threats.

KEY PRODUCT CAPABILITIES

EMPOWER YOUR SECURITY TEAM TO KNOW MORE ABOUT EMERGING THREATS FASTER – IN SECONDS, INSTEAD OF HOURS

- **Fast:** MalQuery is the fastest malware search engine in the security industry, and reduces searches from hours to seconds
- **Precise:** Faster, more accurate results lead to higher quality protection rules for defense against future threats
- **Comprehensive:** CrowdStrike's patent-pending technology indexes terabytes of the latest threat data
- **Increases efficiencies:** Faster malware research streamlines your entire security operations

COMPREHENSIVE TO GENERATE PRECISE RESULTS – YET FLEXIBLE AND EASY TO USE

Use MalQuery for:

- **Fuzzy searching** for sequences of bytes or combinations of byte patterns, including ASCII and Unicode strings
- **Exact searching** to validate all results before returning them to the user
- **YARA hunting** to perform file/sample lookups based on fully featured YARA rules: This feature is orders of magnitude faster than other threat research tools, as it leverages CrowdStrike's unique search technology so queries take a few seconds or minutes instead of hours as with other search engines.

SECURITY PROFESSIONALS AND RESEARCHERS SAVE TIME AND INCREASE PRECISION

- Instant search of byte sequences or byte pattern combinations including ASCII and Unicode
- YARA-based file/sample lookups span the entire history of the collection and the ability to download selected matched samples
- Generates results such as related hashes, malware disposition, file attributes, malware family and adversary attribution with links to Falcon Intelligence reports

SUPPORTED FILE TYPES:

MalQuery is file type-agnostic, and new file types can be added as needed. The system currently indexes all of the following:

Composite Document Files (CDF)
Compiled Java | Dalvik Dex
Microsoft Word (DOC, DOCX) ELF 32/64 bit
Executables (EXE) | Email and HTML
documents | Hangul Word Processor File
(HWP) Java Archive Data | Windows short-
cuts (LNK) Mach-O | PDF | PE32 and PE64 |
Perl script | PowerPoint (PPT, PPTX)
Python script | Python byte compiled
Rich text (RTF) | ASCII text
Microsoft Excel (XLS, XLSX) |
Shockwave Flash (SWF)

CROWDSTRIKE

CONTACT CROWDSTRIKE TO LEARN MORE ABOUT FALCON MALQUERY
1.888.512.8906 | sales@crowdstrike.com