OPSWAT.

DATASHEET

FileScan™

Rapid. In-depth.

Why FileScan?

FileScan is a platform that binds together dozens of state-of-the-art tools, services, and proprietary engines with the focus on Indicators of Compromise (IOCs) and threat extraction from files, documents, scripts and URLs at speed and scale. Using proprietary engines, FileScan is a solution that goes deeper than traditional static analysis tools, providing actionable intelligence in many more cases. Combined with its unmatched speed, it becomes possible to significantly reduce the number of artifacts needing to be sandboxed in an otherwise time-consuming and resource intensive process.

For example, using a cutting-edge unique emulation engine, even extremely obfuscated, state-of-the-art and environment aware malware can be de-obfuscated and dissected in less than 15 seconds. Furthermore, any relevant IOCs (e.g. second stage download files or URLs) are automatically cross-checked with threat intelligence databases to provide accurate attribution.

Coming with a simple RESTful HTTP based API and an open and agile architecture, FileScan offers easy integration into various platforms and corporate systems. The on-premise instance can be deployed on a single server and instantly allows processing of thousands of files/URLs per day. The web interface comes with very user-centric reports that are easy to understand and contain in-depth data if needed.

Verified Technology

Being greatly confident about the robustness of our technology and eager for feedback, we operate a free community service at www.file-scan.io, which is under scrutiny by thousands of daily scans. This field test against fresh malware and phishing threats keeps our solution relevant, hardened and ensures a high level of quality. Being researchers at heart, we often try out cutting-edge technology on the community platform, thereby allowing quick adaption to latest cybersecurity trends. Only proven technology will end up in the enterprise grade commercial product.

Key Features

- Extract Indicators of Compromise (IOCs) from a wide range of executables, documents, scripts, and URLs
- Emulates 90%+ of highly obfuscated state-of-the-art macro malware (VBA), VBS, PowerShell, Jscript, MSHTA, XSL, WSF
- Rapid & deep analysis at high scale (50K+ scans per day/ machine)
- REST API for automated integration
- Integrates with Virus Total, YARA, MITRE ATT&CK framework and more
- Clean and intuitive reports with in-depth data on demand and able to export in HTML, PDF, MISP, STIX
- Simple and cost-effective on-premises standalone deployment or private cloud
- Designed, engineered, and maintained by experienced industry experts

Example Hardware Setup

- Intel Xeon-E 2136 (12M Cache, 3.30 GHz)
- RAM 32GB DDR4 ECC 2666 MHz
- 2x SSD NVMe 256GB RAID

Note: this is an example system that would allow processing 50K files/day with a retention period of 10 days.

Minimal Technical Requirements

- Ubuntu Server 20.04 LTS ("Focal Fossa")
- 8 vCPUs (Preferably 16 vCPUs)
- 16GB RAM (Preferably 32GB)
- 32 GB SSD Disk Space

Throughput / Hardware Requirements

The following table lists explanatory system specs with a retention period of 10 days:

Scans Per Day	Required System CPUs	Required System RAM	Required Storage per Retention Period
1000	4	4GB	256GB
2500	4	4GB	256GB
5000	4	4GB	256GB
10000	8	8GB	256GB
25000	16	16GB	256GB
50000	28	28GB	512GB

Get in Touch

Start your free trial of FileScan at our community platform today. Need more privacy and want to learn about our on-premise offering? Please get in touch at sales@filescan.com.

Engine Features	FileScan	VirusTotal	HybridAnalysis	PEStudio	Manalyze
Render URLs and Detect Phishing Sites	✓	✓			
Extract and Decode Nearly All Malicious VBA Macros	✓		✓		
Analyze VBA Stomped Files Targeted for Any System	✓				
Shellcode Emulation (x86, 32/64)	✓				
Export MISP (JSON) and STIX Report Formats	✓		✓		
Extract and Analyze Embedded PE Files	✓				
Deobfuscate Javascript/VBS	✓		Limited		
Deobfuscate Powershell Scripts	✓		Limited		
Deobfuscate MSHTA Scripts	✓				
Parse METF Embed Equation Exploit Structure	✓				
Parse Malformed RTF Files	✓				
Parse Office Binary File Formats (BIFF5/BIFF8)	✓				
Parse Strict OOXML File Format	✓				
Automatically Decode Embedded Base64 Strings	✓				
Extract Annotated Disassembly	✓				
Decrypt Password Protected Office Documents	✓		✓		
Decompile Java	✓		✓		
Decompile .NET	✓		✓		
Calculate .NET GUIDs (Module Version/TypeLib Id)	✓	✓			
Classify Imported APIs	✓			✓	
MITRE ATT&CK Support (In-report and Search)	✓		✓	✓	
Render PDF Pages	✓	✓	✓		
Extract Embedded Files (eg: OLE2 from Word)	✓	✓	✓		
Automatically Tag Samples Based on Signatures	✓	✓	✓		
YARA Support	✓	✓	✓		✓
Generate Text Metrics (Average Word Size, etc.)	✓				
Detect Cryptographic Constants	✓				✓
Text Analysis (Guessed Language)	✓	✓			

OPSWAT.

Filescan

DATASHEET

Engine Features	FileScan	VirusTotal	HybridAnalysis	PEStudio	Manalyze
Map UUIDs to Known Associated Files / Metadata	✓		Limited		
Filter Strings and Detect Interesting Ones	✓		✓	✓	
Extract and Detect Overlay	✓			✓	✓
Integrated Allowlist	✓	✓	✓		
Detect Alternative IOCs [Emails, Bitcoin Address, etc.]	✓		✓		✓
Calculate Authentihash	✓	✓	✓		
Verify Authenticode Signatures	✓	✓	✓	✓	
Parse RICH Header	✓	✓	Limited	✓	✓
Calculate Entropy of Resources	✓	✓		✓	✓
Detect URLs, Domains and IP Addresses	✓	Limited	✓	✓	✓
Calculate Hashes of Resources	✓	✓		✓	✓
Calculate Imphash	✓	✓	✓		✓
Calculate SSDEEP	✓	✓	✓		✓
Extract PDB Information	✓	✓	✓	✓	
Detect TLS Callbacks	✓		✓	✓	✓
Resolve Known Import Ordinals to Names	✓		✓	✓	✓
Detect Anomalies [eg: Header Checksum Validation]	✓	Limited	✓	✓	✓
Query VirusTotal for Reputation Checks	✓	✓	✓	✓	✓
Detect Packers [PEiD]	✓	✓	✓	✓	✓
Detect File Types	✓	✓	✓	✓	✓
Calculate Hashes of Sections	✓	✓	✓	✓	✓
Calculate Entropy of Sections	✓	✓	✓	✓	✓
Extract Strings from Executable	✓	✓	✓	✓	✓
Extract/Detect Resources	✓	✓	✓	✓	✓
Extract/Detect PKCS7 Certificate	✓	✓	✓	✓	✓

OPSWAT.

Protecting the World's Critical Infrastructure