

FileScan.IO Feature Comparison					
Feature	FileScan.IO	VirusTotal	HybridAnalysis	PEStudio	Manalyze
Extract and decode nearly all malicious VBA macros	Yes	No	Yes	No	No
Analyze VBA stomped files targeted for any system	Yes	No	No	No	No
Extract & analyze embedded PE files	Yes	No	No	No	No
Deobfuscate Javascript / VBS	Yes	No	Yes, but limited	No	No
Deobfuscate Powershell scripts	Yes	No	Yes, but limited	No	No
Deobfuscate MSHTA scripts	Yes	No	No	No	No
Parse Office binary file formats (BIFF5/BIFF8)	Yes	No	No	No	No
Parse Strict OOXML file format	Yes	No	No	No	No
Automatically decode embedded Base64 strings	Yes	No	No	No	No
Extact annotated disassembly	Yes	No	No	No	No
Decrypt password protected office documents	Yes	No	Yes	No	No
Decompile Java	Yes	No	Yes	No	No
Decompile .NET	Yes	No	Yes	No	No
Calculate .NET GUIDs (Module Version/TypeLib Id)	Yes	Yes	No	No	No
Classify imported APIs	Yes	No	No	Yes	No
MITRE ATT&CK support	Yes	No	Yes	Yes	No
Render PDF pages	Yes	Yes	Yes	No	No
Extract embedded files (e.g. OLE2 from Word)	Yes	Yes	Yes	No	No
Automatically tag samples based on signatures	Yes	Yes	Yes	No	No
YARA support	Yes	Yes	Yes	No	Yes
Generate text metrics (average word size, etc.)	Yes	No	No	No	No
Detect cryptographic constants	Yes	No	No	No	Yes
Text analysis (guessed language)	Yes	Yes	No	No	No
Map UUIDs to known associated files / meta-data	Yes	No	Yes, but limited	No	No
Filter strings and detect interesting ones	Yes	No	Yes	Yes	No
Extract and detect overlay	Yes	No	No	Yes	Yes
Integrated whitelist	Yes	Yes	Yes	No	No
Detect alternative IOCs (E-Mails, bitcoin address, etc.)	Yes	No	Yes	No	Yes
Calculate authentihash	Yes	Yes	Yes	No	No
Verify authenticocode signatures	Yes	Yes	Yes	Yes	No
Parse RICH header	Yes	Yes	Yes, but limited	Yes	Yes
Calculate entropy of resources	Yes	Yes	No	Yes	Yes
Detect URLs, Domains and IP addresses	Yes	Yes, but limited	Yes	Yes	Yes
Calculate hashes of resources	Yes	Yes	No	Yes	Yes
Calculate lmp hash	Yes	Yes	Yes	No	Yes
Calculate SSDEEP	Yes	Yes	Yes	No	Yes
Extract PDB information	Yes	Yes	Yes	Yes	No
Detect TLS callbacks	Yes	No	Yes	Yes	Yes
Resolve known import ordinals to names	Yes	No	Yes	Yes	Yes
Detect anomalies (e.g. header checksum validation)	Yes	Yes, but limited	Yes	Yes	Yes
Query VirusTotal for reputation checks	Yes	Yes	Yes	Yes	Yes
Detect packers (PEiD)	Yes	Yes	Yes	Yes	Yes
Detect file types	Yes	Yes	Yes	Yes	Yes
Calculate hashes of sections	Yes	Yes	Yes	Yes	Yes
Calculate entropy of sections	Yes	Yes	Yes	Yes	Yes
Extract strings from executable	Yes	Yes	Yes	Yes	Yes
Extract/Detect resources	Yes	Yes	Yes	Yes	Yes
Extract/Detect PKCS7 certificate	Yes	Yes	Yes	Yes	Yes

Version 1.0-1013