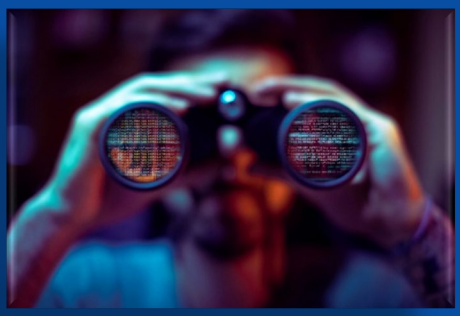
FILESCAN.IO THREAT INTELLIGENCE CHEAT SHEET



In this document, we showcase some of the diverse threat hunting capabilities available in the advanced search feature:

https://www.filescan.io/advanced-search

Malicious Documents

Office Files with Foreign Language and Active Content:
https://www.filescan.io/search-result?filetype=ms-office&verdict=malicious&tag=macros-on-open&unique_files=false&method=and&signal_groups=TXT000

Office Files using default Symmetric Key Encryption:
https://www.filescan.io/search-result?filetype=ms-office&verdict=malicious&tag=velvetsweatshop&unique_files=false&method=and

Office Files utilizing the EMBED.Equation exploit:
https://www.filescan.io/search-result?filetype=ms-office&verdict=malicious&unique_files=false&method=and&signal_groups=EMU005

Office Files with Auto-Execution and Process Spawns:
https://www.filescan.io/search-result?filetype=ms-office&verdict=malicious&tag=macros-on-open&unique_files=false&method=and&signal_groups=EMU006

Phishing PDFs:
https://www.filescan.io/search-result?verdict=malicious&tag=phishing&rate_from=5&unique_files=false&method=and&signal_groups=PDF000

Suspicious Executables

Packed PE files with process hollowing capabilities:
https://www.filescan.io/search-result?filetype=exe&verdict=malicious&tag=packed&unique_files=false&method=and&signal_groups=SIG006

PE file with a RDTSC timing instruction:
https://www.filescan.io/search-result?filetype=exe&verdict=malicious&unique_files=false&method=and&signal_groups=DS002

FILESCAN.IO THREAT INTELLIGENCE CHEAT SHEET

Unusual File Types

Malicious Windows Shortcut Files spawning rundll:
https://www.filescan.io/search-result?filetype=lnk&verdict=malicious&tag=rundll32&unique_files=false&method=and

Malicious files delivered via VHD image files:
https://www.filescan.io/search-result?verdict=malicious&tag=vhd&unique_files=false&method=and

Mobile Threats

Malicious APKs:
https://www.filescan.io/search-result?filetype=apk&verdict=malicious&rate_from=5&unique_files=false&method=and&signal_groups=A001

APKs reading the device ID (IMEI):
https://www.filescan.io/search-result?filetype=apk&verdict=malicious&rate_from=5&unique_files=false&method=and&signal_groups=DC001

Malicious Web Threats

E-Mails containing macro-enabled attachments:
https://www.filescan.io/search-result?filetype=mail&verdict=malicious&tag=macros&unique_files=false&method=and

Phishing URLs:
https://www.filescan.io/search-result?source_type=url&verdict=malicious&tag=phishing&unique_files=false&method=and

Additional Resources

Threat Feed: https://www.filescan.io/api/feed/atom
Personal Threats Overview Page: https://www.filescan.io/threats-overview
API Documentation: https://www.filescan.io/api/docs
CLI for API (pip package): https://github.com/filescanio/fsio-cli

filescan.io
RAPID. IN-DEPTH.