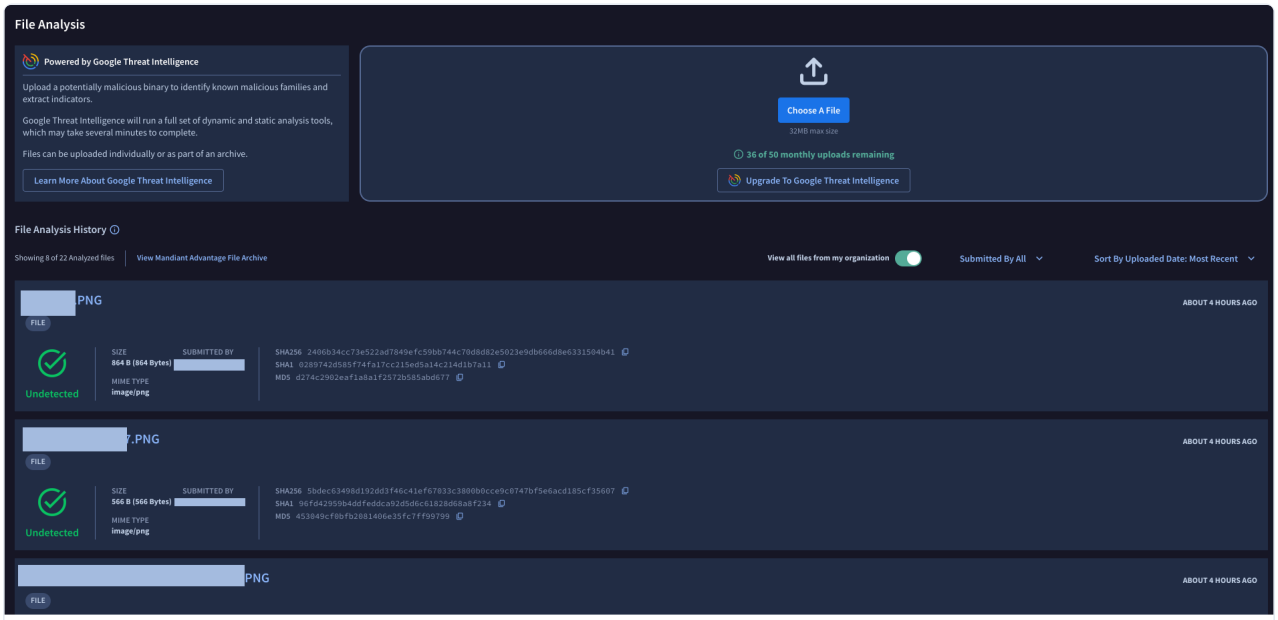
FILE ANALYSIS

File Analysis allows you to upload a potentially malicious binary to identify known malicious families and extract indicators. Mandiant Advantage Threat Intelligence (MATI) runs a comprehensive set of dynamic and static analysis tools that can take several minutes to complete. You upload files for analysis individually or as part of an archive.

> The File Analysis page shows a **Powered by Google Threat Intelligence** heading. That means Google Threat Intelligence produces a private scanning verdict that is accessible to you in MATI.
> See **Actionable threat intelligence at Google scale** **(https://cloud.google.com/security/products/threat-intelligence?hl=en&e=48754805)** to learn more about expanding automated file analysis with Google Threat Intelligence.



File Analysis landing page in MATI, showing File Analysis History with example files that are uploaded and analyzed

Internally, private scanning analyzes files and URLs with Google Threat Intelligence in a privacy-preserving fashion. Files and URLs uploaded through this offering won't be shared with anyone beyond your organization, and remain in MATI for a brief period of time. The resulting analyses are ephemeral and only visible to users in your MATI organization.

> Private analyses don't contain antivirus verdicts. They only contain the output of all the other characterization and contextualization tools that we run, including sandboxes.

Our sandboxes, detection tools, and configuration extractors will process most file types including:

- Executables: Windows, Mac, Linux
- Scripts: Powershell, bat, vbscript, jscript
- Document files: doc(x), ppt(x), xls(x), pdf, rtf
- Email: eml, msg
- Compressed archives: iso, rar, zip, 7z

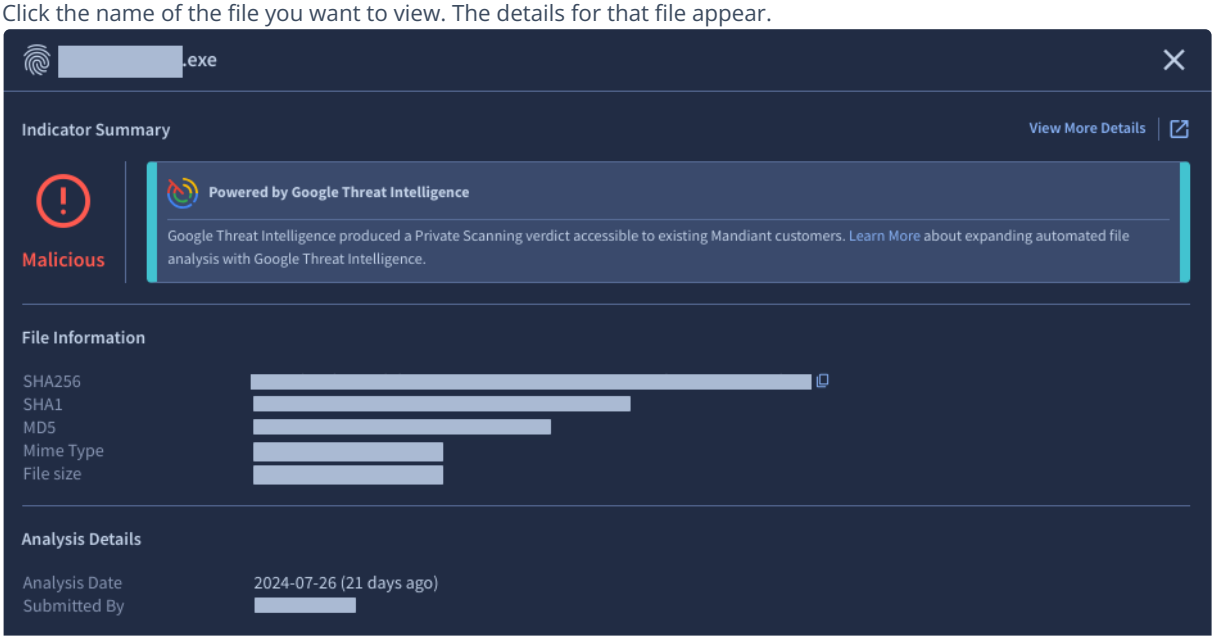
- You can upload up to 100 files monthly. Your remaining total is displayed on the File Analysis landing page.
- The file size limit 32 MB.
- Include only a small number of files in the compressed archives to get better results.
- Upload files to analyze with their original file extension. This helps some of our tools to process the file correctly.

Upload a file for private scanning

1. From MATI, go to **File Analysis** and then click **Choose a File**.
2. Select the file you want to upload and click **Open**. The screen that appears lets you know which servers the file is stored on and when it's going to be deleted after analysis.
3. Optional: Modify the **Filename** value if you need to correct any details, such as an incorrect file extension.
4. Optional: If the file you're uploaded in encrypted, enter the password to decrypt your file.
5. Click **Analyze File**. A new entry for the file appears. The status is updated after the file is analyzed.

View file analysis details

1. From MATI, go to **File Analysis**.
2. Filter the file list by any of the following:
    - **View all files from my organization**
    - **Submitted By**
    - **Sort By Uploaded Date**
3. Click the name of the file you want to view. The details for that file appear.

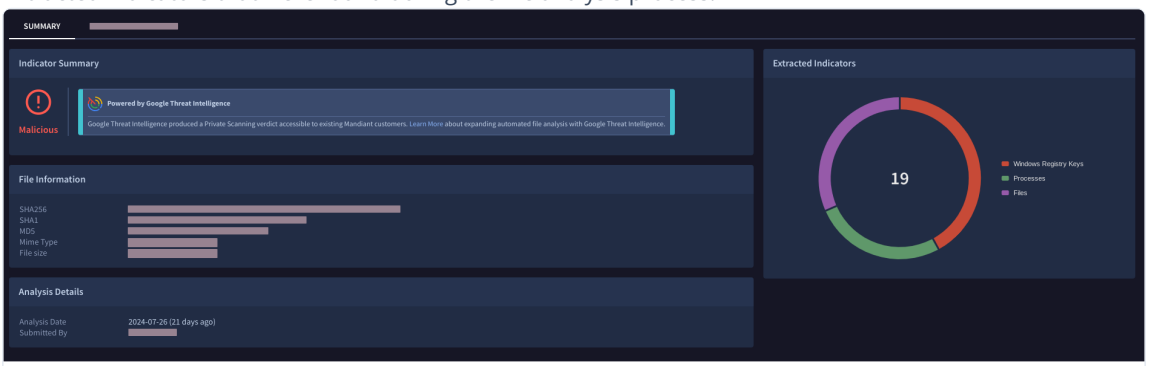


Example files analysis on an .exe file that resulted in a Malicious indicator summary

4. Note the details for the file:
    - **Indicator Summary**: Shows the results of the file analysis (Undetected or Malicious).
    - **File Information**
        - **SHA256**: Hash value of the file that uses the SHA256 algorithm.
        - **SHA1**: Hash value of the file that uses the SHA1 algorithm.
        - **MD5**: Hash value of the file that uses the MD5 algorithm.

        - **Mime type**: Indicates the nature and format of the file.
        - **File size**: Shows the file size in MB/KB and bytes.
    - **Analysis Details**
        - **Analysis Date**: The date when the automated analysis was completed.
        - **Submitted By**: Which user in your organization submitted the analysis request.

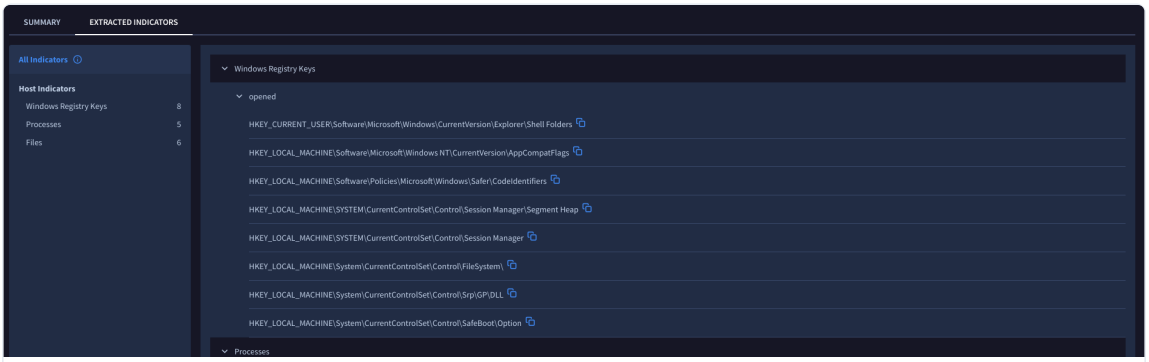
5. Click **View More Details** to open the File Analysis details in the same tab or click to open the details in a new tab. The following options appear:
    - **Summary**: Provides the File Analysis details from the preceding screen, as well as an interactive graph of any Extracted Indicators that were found during the file analysis process.



Summary tab for an analyzed file, including Extracted Indicators

    - **Extracted Indicators**: Provides a categorized list of extracted indicators and more details about them.

> Listed indicators are derived from static and dynamic analysis for the selected file. The indicators may or may not be associated with malicious behavior.



Extracted Indicators tab listing Host Indicators: Windows Registry Keys, Processes, and Files

View Mandiant Advantage file archive

Follow these steps if you need to access details files that were analyzed prior to automated private scanning.

1. From MATI, go to **File Analysis** and then click **View Mandiant Advantage File Archive**.
2. Filter the file list by any of the following:
    - **View all files from my organization**
    - **Submitted By**
    - **Sort By Uploaded Date**

3. Click the file name to open its Indicator Summary view.
4. Click **View More Details** to open the File Analysis details in the same tab or click to open the details in a new tab.
5. Optional: Click **Ask an Expert** to request further research on the file. A screen appears for you to provide a brief description of the situation, including what is most critical, a timeline of events, and what feedback report you expect from the expert analyst team. You may upload supporting evidence as needed. Responses may take up to 48 hours.