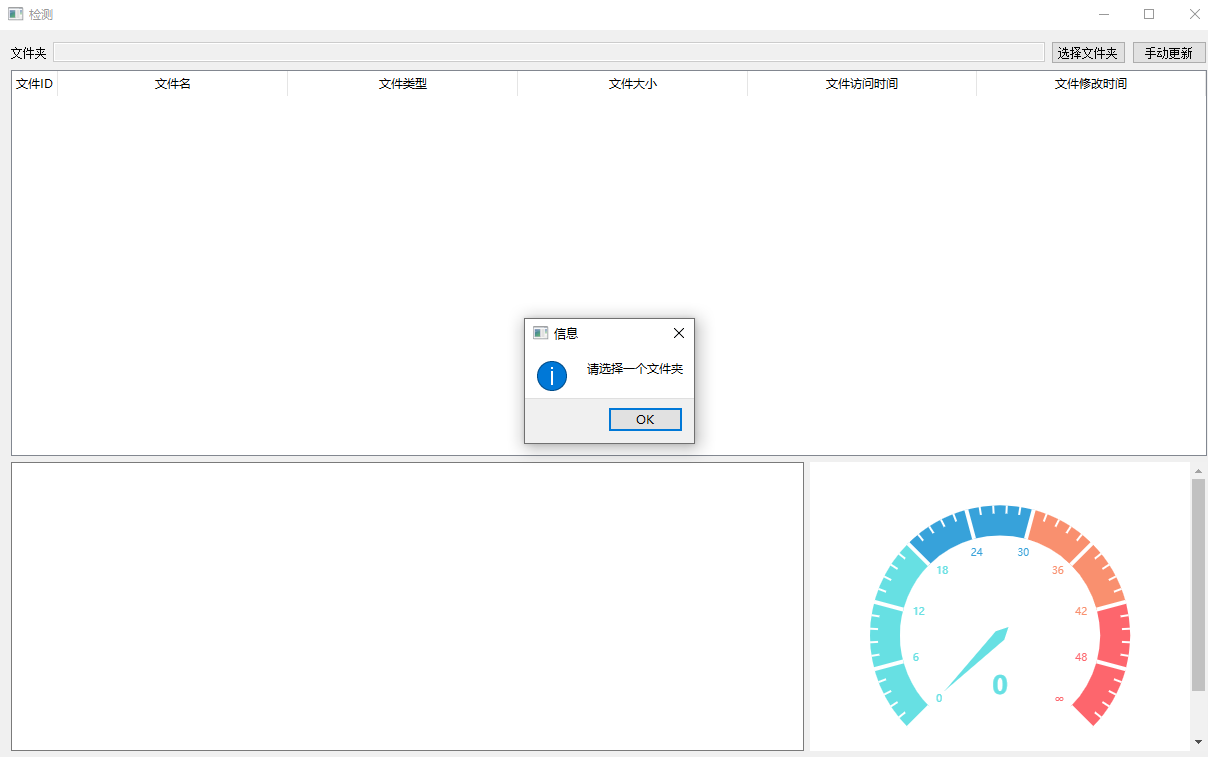
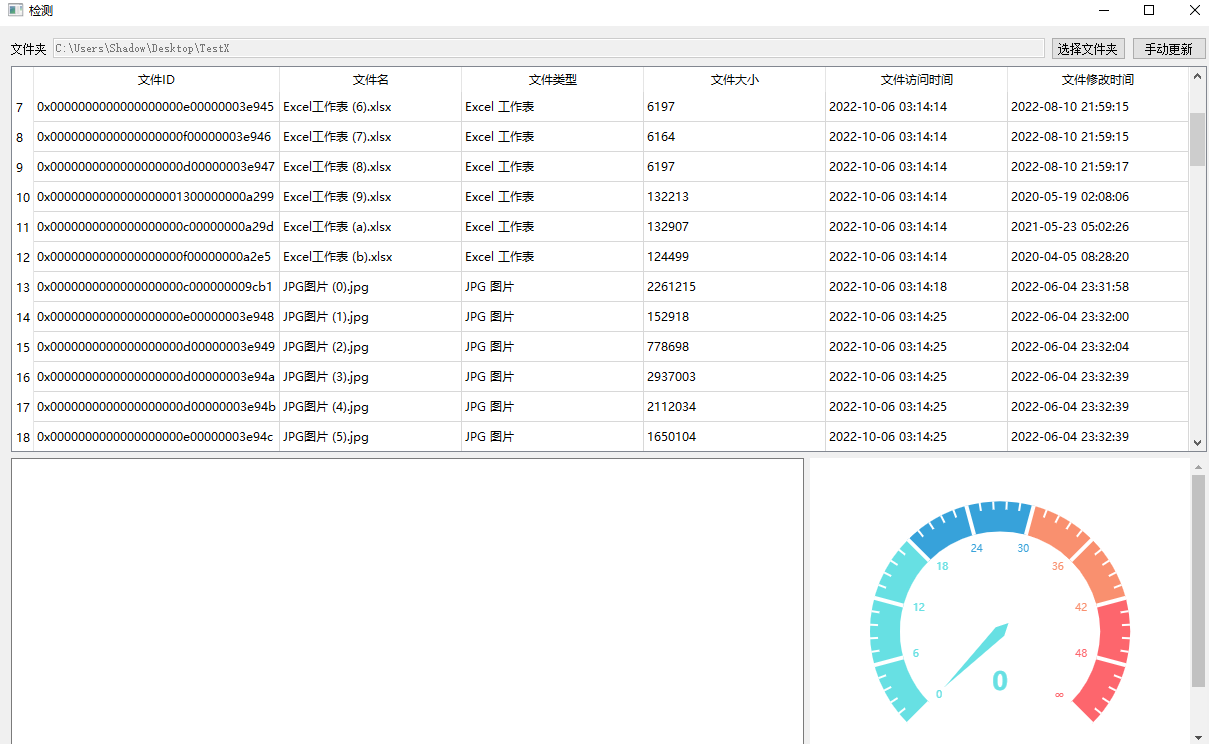
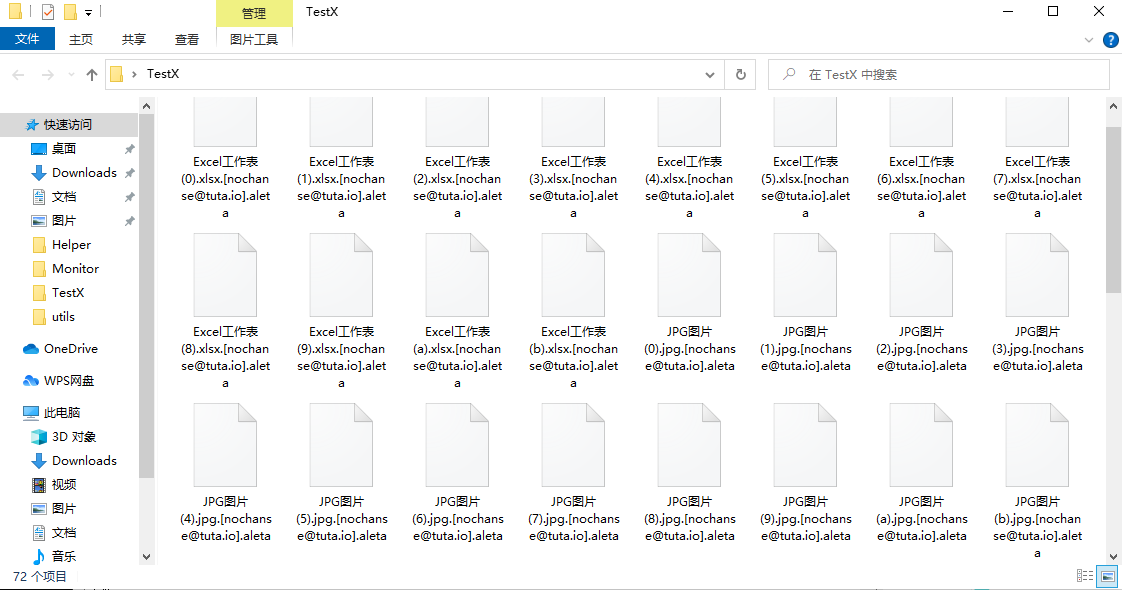
1. Start the program without selecting a folder:



1. Enable the file detection system and select the specified folder to monitor (the designated target folder includes twelve files that may be infected by ransomware, including txt, jpg, png, docx, xlsx, and pdf), and wait for file changes.

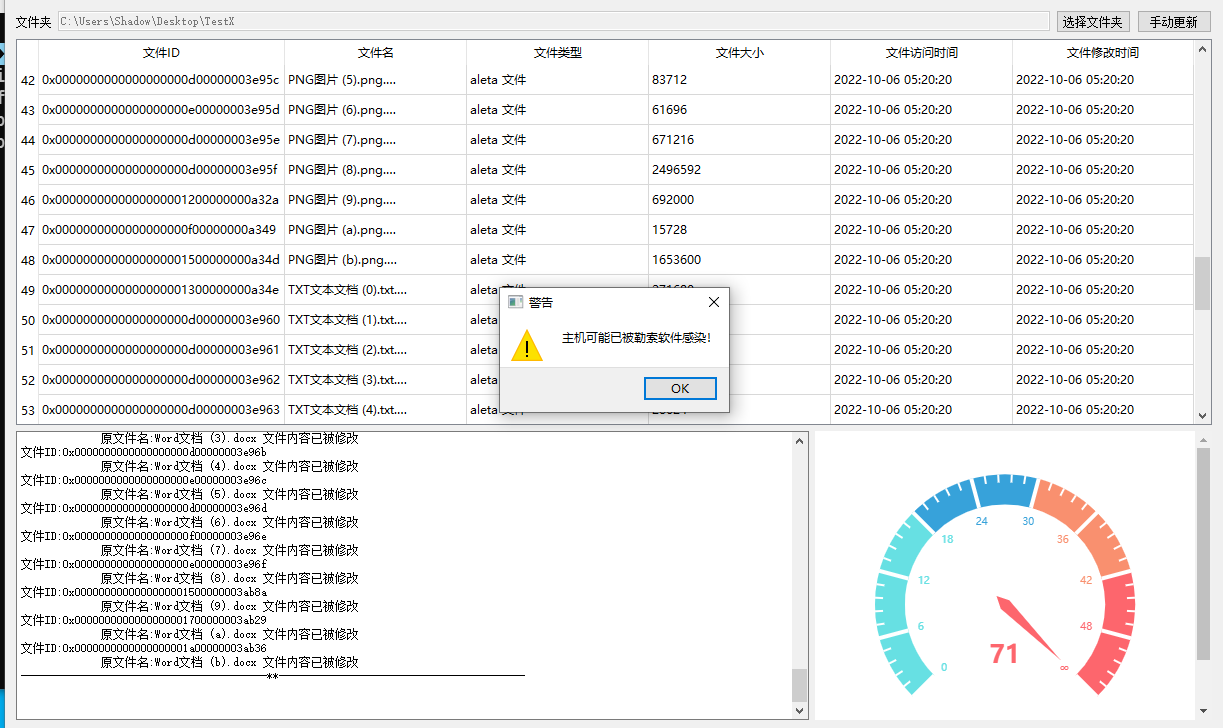


1. Run ransomware virus in the virtual machine. During testing, use the sample "Ransomware.Eleta\_1". After running the ransomware software, all files in the trap folder are encrypted, and the access time and modification time of batch files change within a short time (1 second). The file type (file extension) is modified to [nochanse@tuta.io].aleta. The files in the specified folder are infected. All folders are encrypted.



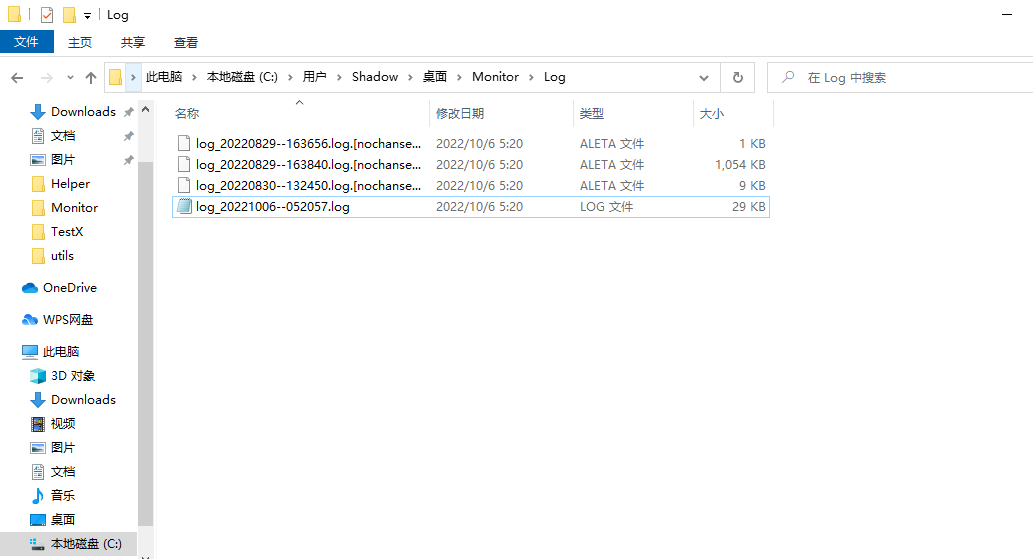


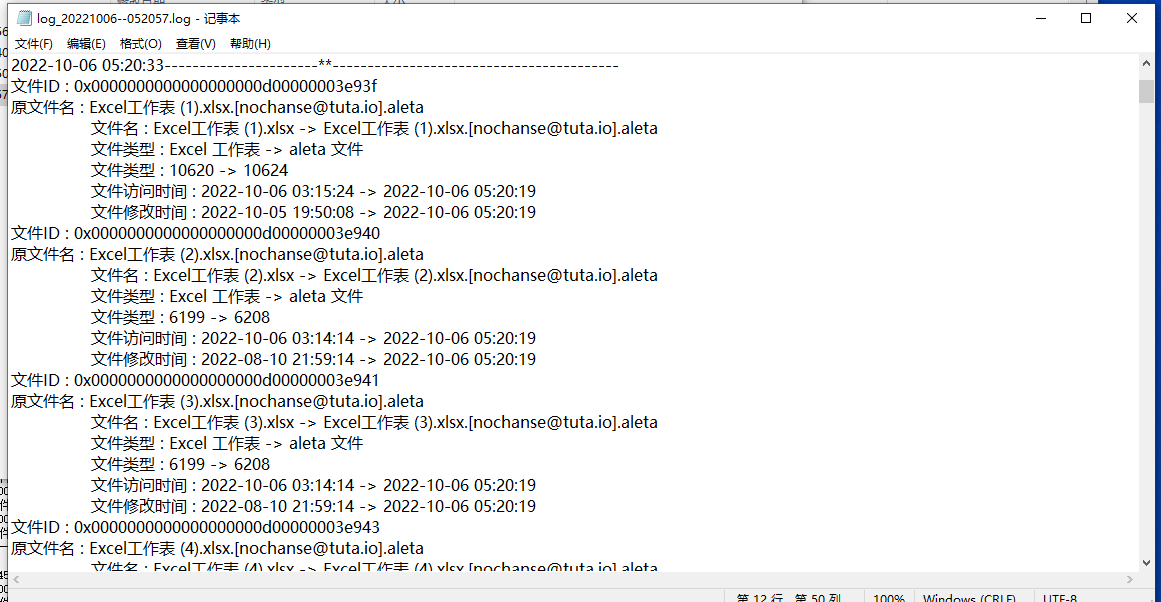
1. The system detects that out of 72 files, 71 files have undergone a change in status within 1 second, exceeding the average threat level (43) of systems infected by different ransomware. The program issues an alert, and the dashboard also points to the corresponding location, providing a more intuitive view of the status of the monitored folder.



1. While the program is running, a log file is generated in the project root directory. The log file is loaded every time the program runs, and the current changes in the monitored folder are appended to the log file. This includes recording changes in file modification time, access time, size changes, file name changes, and type changes. When the log file size exceeds a certain limit (1M), a new log file is created. Considering that the log file may be encrypted, before writing to the log, check if the log file is infected. If infected, create a new log file according to the log file naming format.

Log folder.





Log content. New log files created after exceeding 1M.

