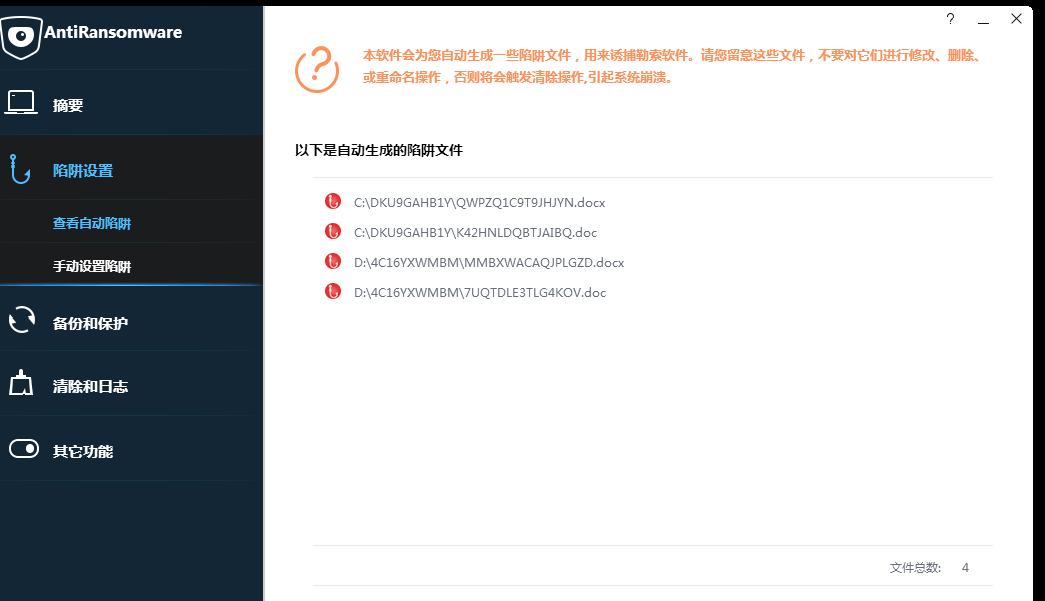
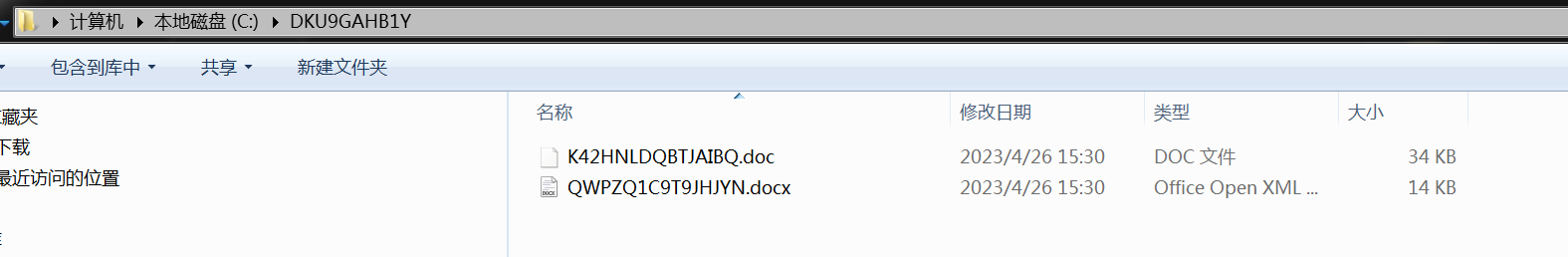
**AntiRansomware Notes**



Screenshot of the automatic decoy file system



C disk automatic bait file screenshot

The user manually set the bait file. This time, a test file on the desktop was successfully dragged into the interface, directly showing its file path, and the function test was successful.

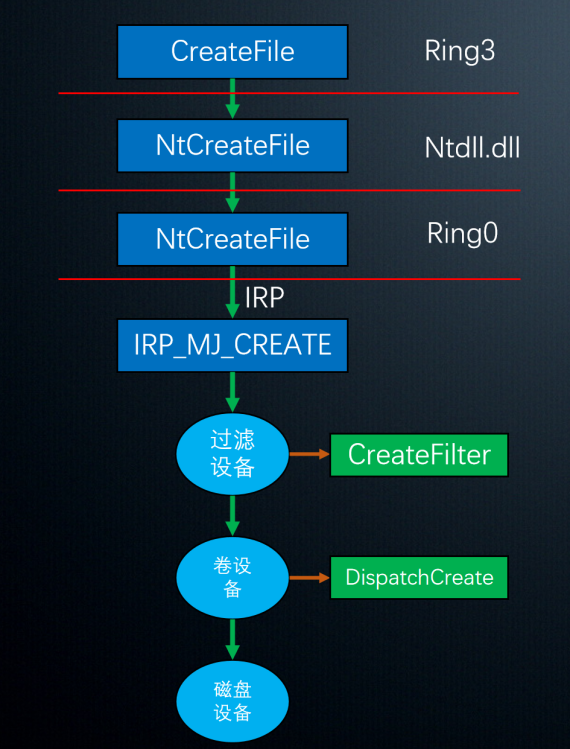


Screenshot of the manual decoy file system

Drive module process

SFilter Framework process

Windows Structure is divided into ring3-ring0 (user layer-kernel layer) structure, the createfile api for example, the api for ring3 layer, by constantly tracing the underlying call to ring0 layer NtCreateFile, the system SFilter file filtering frame is connected between Ring0 layer and virtual devices, filtering device is the design of the file filtering frame, need and volume device binding, and volume device and corresponding to the host disk, such logical connection is the overall framework. Messages preferentially filter through the device and then through the roll device with the disk device.

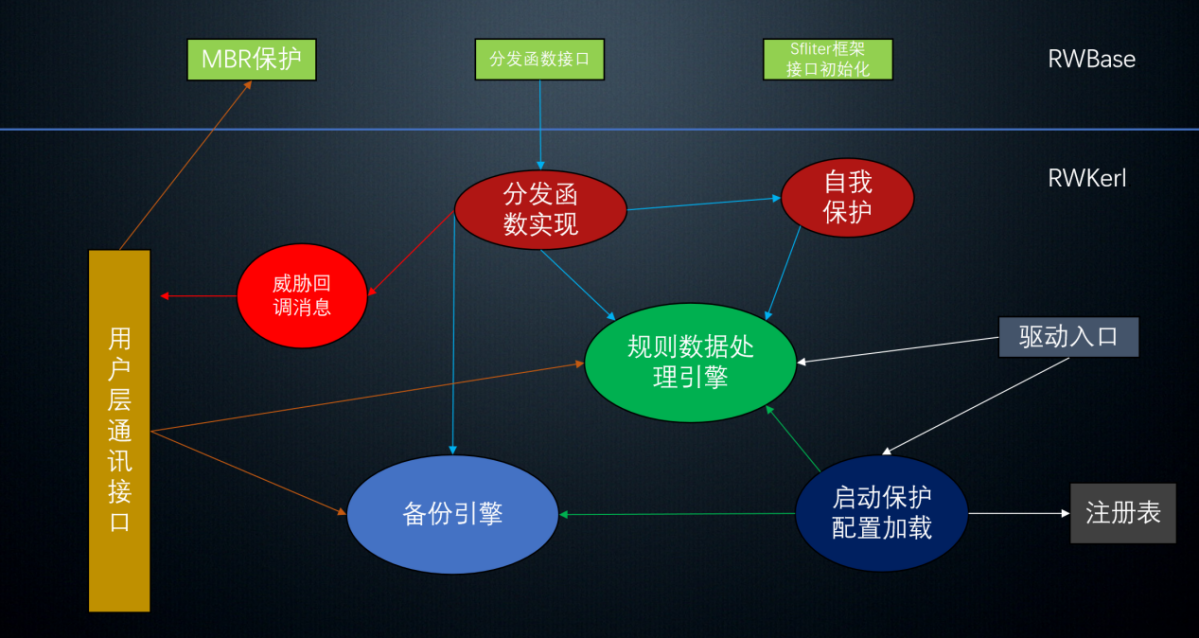


SFilter Framework diagram



Filter device-roll device-disk device relationship diagram

Drive module framework



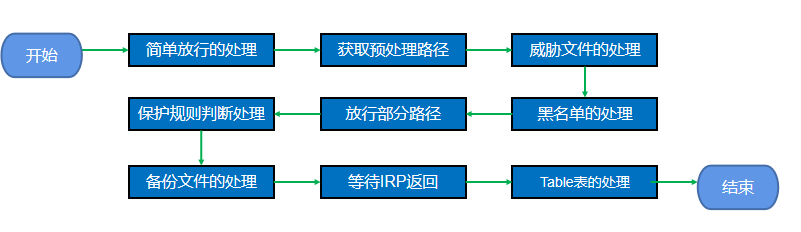
The RWBASE-RWKERL relationship diagram

The drive module of this design is divided into two parts, respectively, RWBase (basic module) and RWKerl (business module), basic module provides the basic filtering drive framework and distribution function interface, and the actual part is implemented in the business module, such as the implementation of distribution function, rule processing, configuration loading, backup engine and other backup. Such a design of framework and business separation is helpful for future function maintenance and upgrade. Developers can only write functions in the modules of the business, without considering some of the basic modules and framework, and reduce the development cost and time.

Distribution function design process

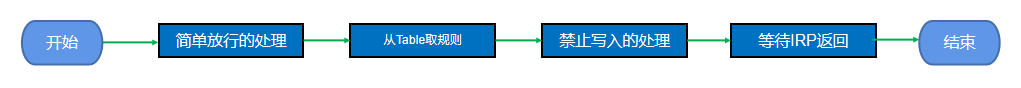
The design of the distribution function is the key in the driver module, equivalent to rules to constrain the final file filtering implementation. There are 4 distribution functions Create, Write, SetInformation, DirectoryControl.

Create, First get some preprocessing profile path, and then the restart lock clear threat file processing, followed by the processing of the blacklist, release the path of some system resources (because the system itself, and the ransomware will not read these folders, so choose release), then judge the protection rules, whether to read and write the large files in the protection directory, then process the backup files, then wait for the lower device IRP, finally stored in the Table table. In addition, the Table table is a table used by all distribution functions to storing file objects and other content.



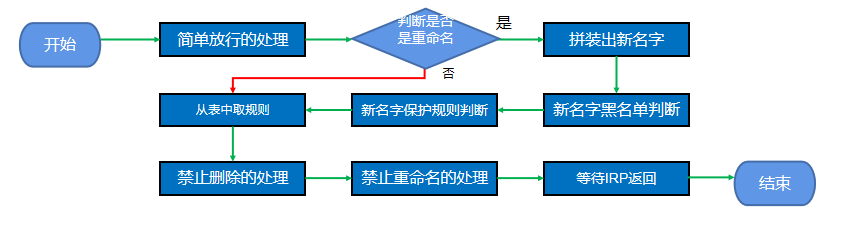
Create Flow chart of distribution functions

Write, Write manages the file write operation, get the rules from the table, then judge and prohibit the written operation, and then wait for the IRP of the lower device to return.



Flow diagram of the Write Distribution functions

SetInformation, The distribution function is the operation of renaming, first determine whether the renaming operation, not directly in the table, if it is renamed operation then the pretreatment splicing new name to blacklist judgment, protection rules, if all do not exist then continue to table table take objects and then ban the delete, renaming, and finally wait for the lower device IRP return.



SetInformation Flow chart of distribution functions

DirectoryControl, The distribution function implements the hidden function of the file path, and the hidden implementation of the previous backup path is implemented in the RING 0 layer through the distribution function.

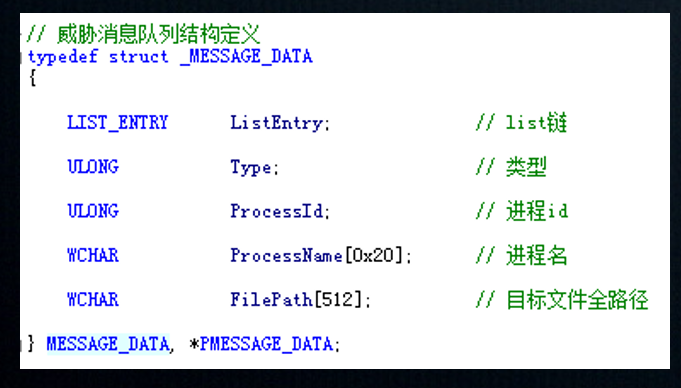


DirectoryControl Flow chart of distribution functions

Threat message processing process

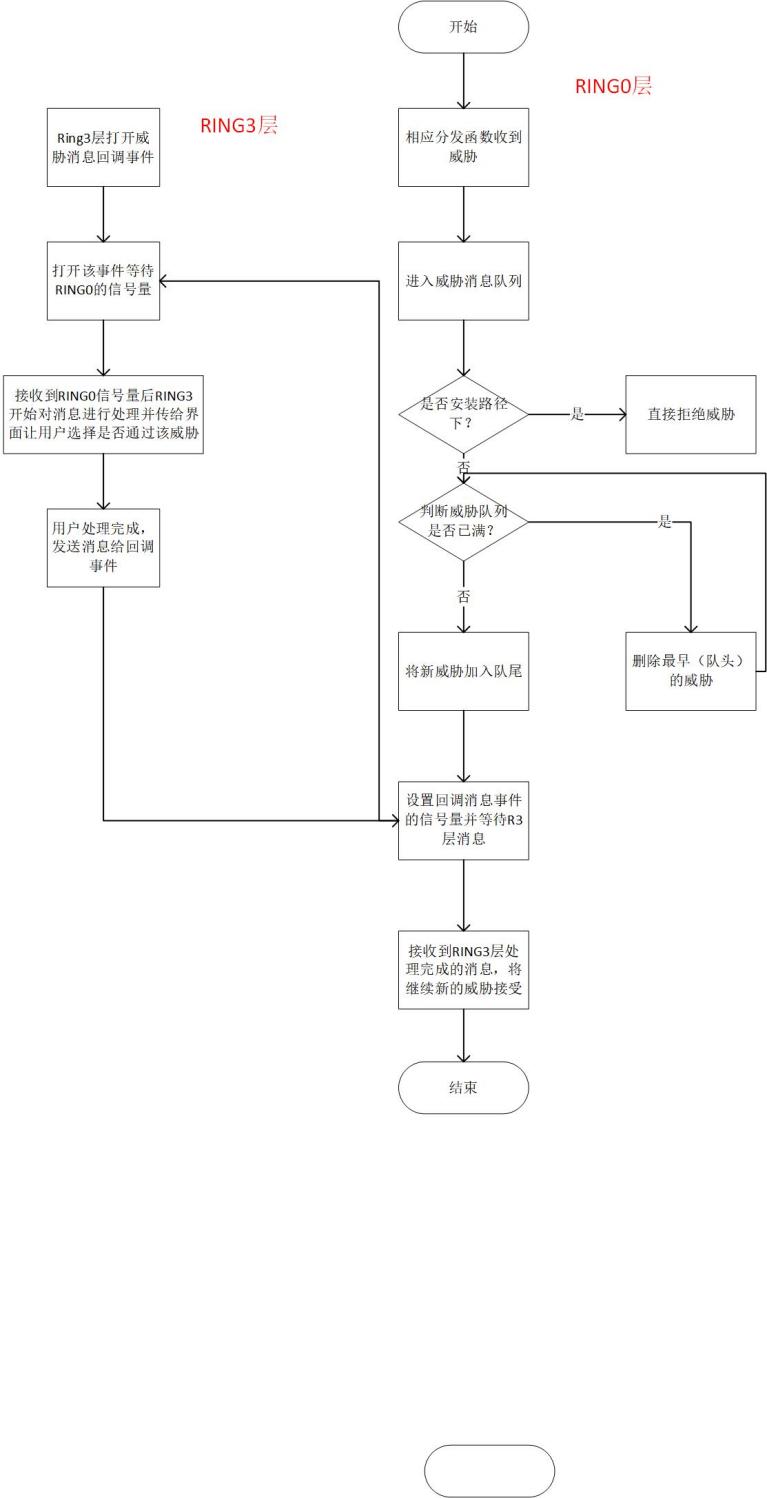
Threat message processing is the whole process between the RING 0 layer processing to complete the pop-up prompts sent to the RING 3 layer user interface.

Threat messages have a threat message queue for, recording the process name and ID of the threat process and the threat file path.



Threat message queue structure definition

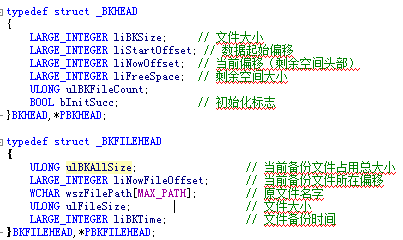
From the incoming threat queue of threat-qualified suspected threat files intercepted by the distribution function, first determine whether the threat comes from the installation directory of the system, and then directly prevent the nonincoming threat queue. Then determine whether the threat queue is full. If it is full, delete the earliest threat of the queue head, then send the new threat to the end of the queue, set the signal volume of the callback message and wait for the reply message of the RING 3 layer. This RING 3 layer waiting signal after receiving the corresponding to the message, the message to the user interface threat for user choose whether to release or processing, finally user processing is completed, RING 3 through callback event signal to RING 0 waiting event, RING 0 processing event will continue to process the new threat, to reciprocating.



Threat message RING 0-RING 3-layer processing process

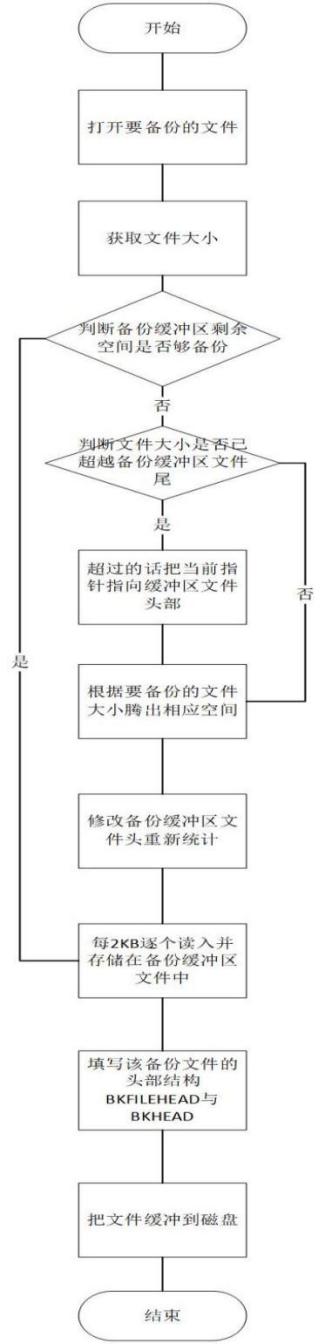
Backup operation processing process

The backup module of this design adopts circular backup. In structure, if the backup queue is filled, the required backup content will be filled in from scratch, so that the backup operation will be recycled.



Backup queue structure

Backup core logic idea is to open the backup file and get the file size, and then determine whether the backup buffer remaining capacity enough to backup the file, 1) if not meet, judge the file size can meet the end of the end of backup buffer, the file first fill the end, then put the current pointer from the end to the head of the buffer file, and then make corresponding space according to the size of the backup file, modify the buffer file head (the file head value for the data starting offset value). Then do the 2) operation.2) Gradually read into the backup buffer every 2 KB, then fill in the backup file header (BKFILEDHEAD) structure and modify the cache file header, and finally update the file buffer to the disk to complete the backup operation.



Flow chart of the backup processing

The third function is backup and protection function, backup setting sub-interface can view the current selected backup disk and other disk information, users can change the interface, and can view the disk space size divided to the backup, the bottom can modify the file backup threshold, by clicking the required threshold (25M-300M).



small paper

Big file

A screenshot of the backup configuration system

Users can click on the lower left of the interface to add file function, and then drag and drop the file into the list area, so can enter the file for the file protection function, also can delete already protected file (modify file same trigger protection), at the same time if the list of files large this function also support fuzzy query.



Screenshot of the large file protection system

Here you can view the file extensions already in the rule base, and users can delete backup types and add custom extensions. All files that meet the backup type and are within the backup limit will be backed up to the backup directory when they are modified, renamed, or deleted.

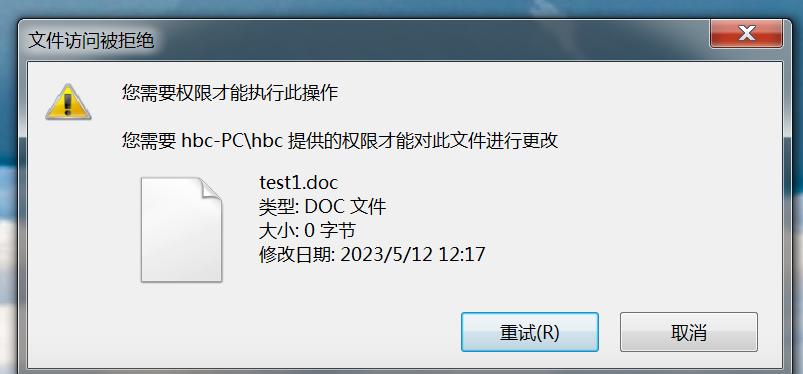


Backup type system screenshot

Use test file for file protection test, when we take a delete operation to the test in the protected, the defense system will conduct a threat popup to prompt the user whether to release the operation, if cancel, block the operation, if you need to release, you need to enter the system password and then click the sure button.



Screenshot of the file operation warning pop-up system

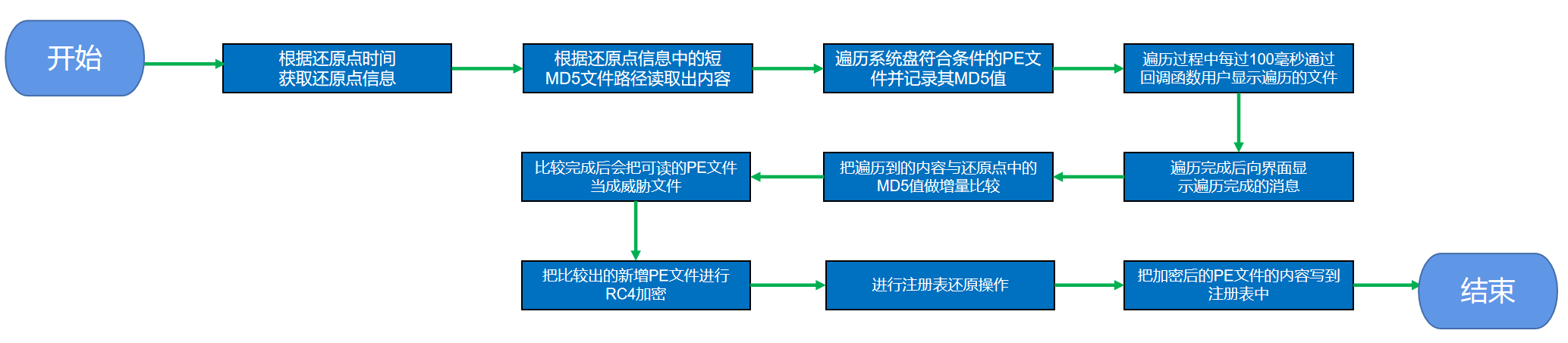


Test sample screenshots

Restore the clearance process

Restore the running process of the calculation

By restoring the point time corresponds to the information of the restore point, the reduction point time is equivalent to an identification ID, and then read out the content according to the MD5 file path in the restored point information, then go through the disk to find the qualified PE file and record the MD5 (in the process of constantly synchronized to view the user interface through the callback function). Then compare the md 5 value with the reduction point md 5 value, write the new suspected threat file PE in the file and encrypt RC4 (prevent it from continuing external threat and being eliminated by other processes), continue the registry restore operation, and write the encrypted suspected file into the registry.



Restore the point calculation flow chart

To restore the clear, the manual clear part can view the existing restore point creation time, the lower left can set the restore point generation parameters, such as the restore point generation interval time, and the maximum number of restore point saved (considering the system storage resources).

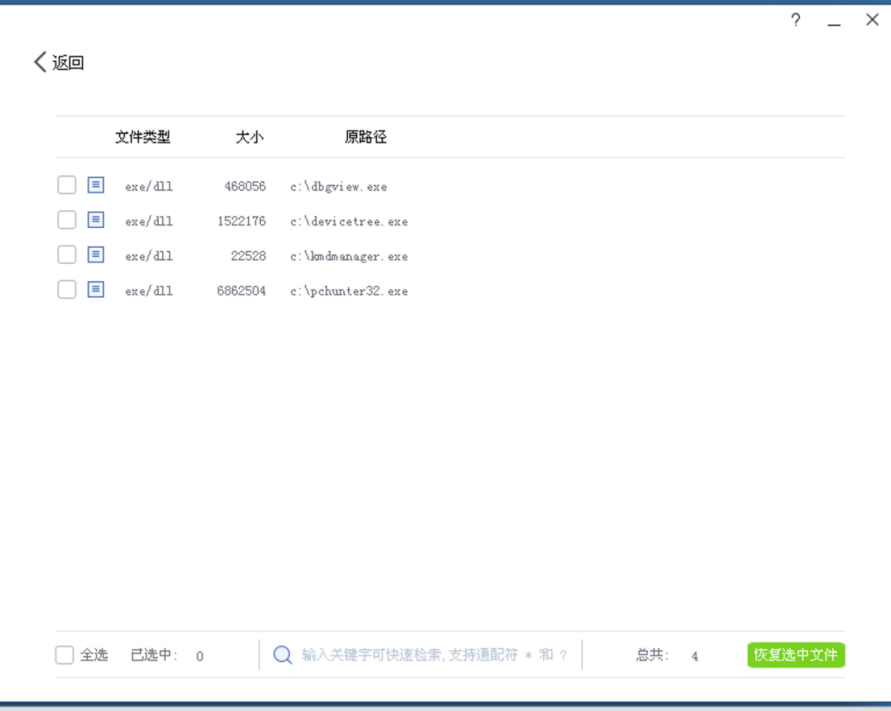


Restore the point system screenshot



Restore the point generation configuration screenshot

All the contents in the clear log list, including the clear time, the total size and number of files, click the view button to view all the files cleared each time, and you can see all the files suspected of being deleted. Users can check the files deleted by the system for recovery operation.



Clear the log list screenshot

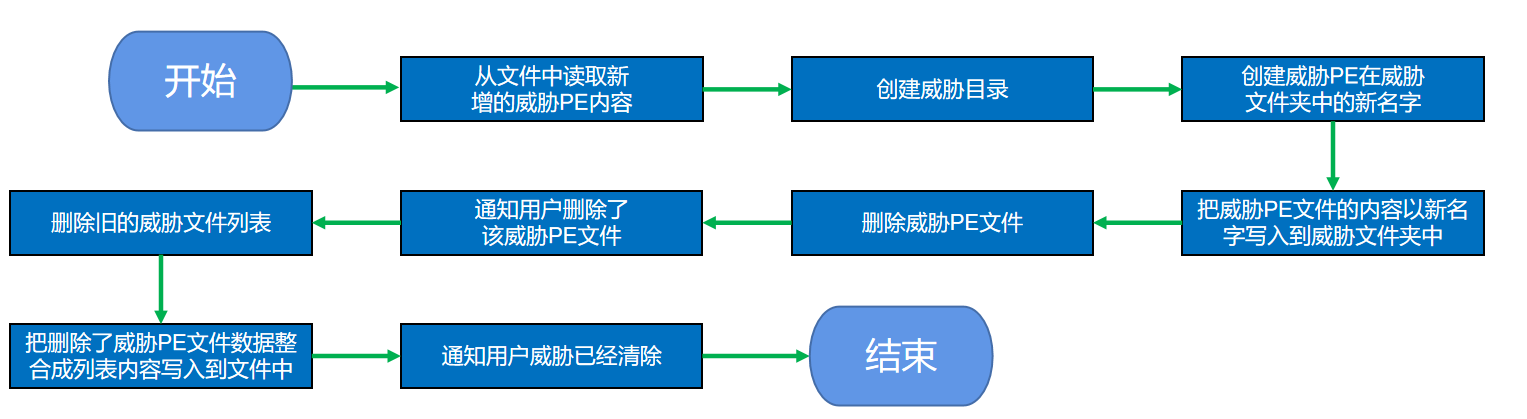
The next step is to test the process of restoring and clearing when the threat invasion. When the trap file is triggered, the threat warning window will pop up, showing the name and number of the salted fish process, and prompt the user to save the work content file to the only folder that can be written. Then select the restore point that already exist to restore the clear process.



Restore the point to trigger the warning screenshot

Restrestart clearing process

After the system restart, create the threat directory, and read the new PE file into the directory and renamed, then notify the user to delete the threat PE file, then delete the threat file list, at the same time synchronization just deleted threat file PE list to the interface allows the user to view and restore the mistakenly deleted files.



Clear the flowchart after the restart

Then four pop-up processes to generate a snapshot of the file, lock the suspected threat PE file by comparison, and then restore the registry and then restart the host system.



Screenshot of the restoration process

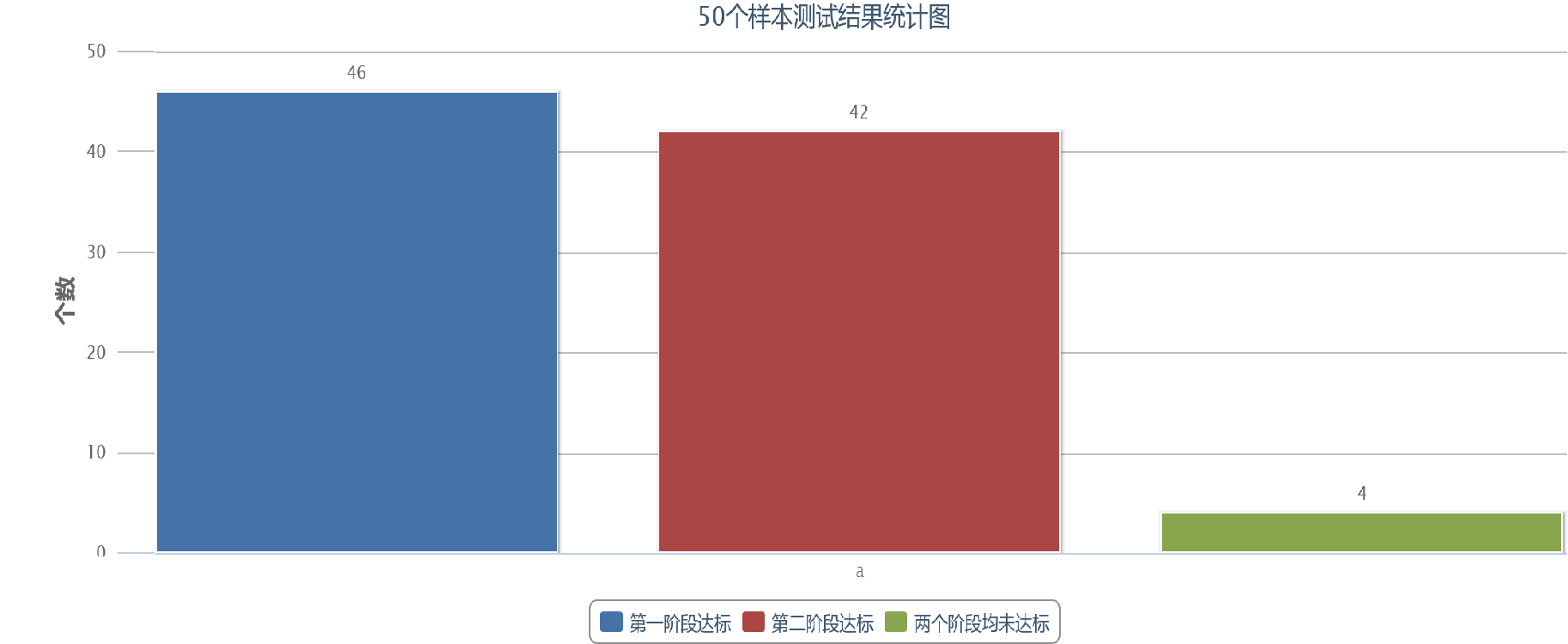
After the restart, the system popup prompts to clear all the complete file paths, and the user can restore the mistakenly deleted files in the clear log.



Threat file clear screenshot

System defense effect

Divide the defense into two levels, degree 1 to detect the ransomware and then return to the interface to prompt the user. Defense degree 2 can block in 1 and can clear the threat file function after restart. To meet the requirements of defense degree 1 or 2, and to fail to meet the requirements of defense degree 1 or 2.



Statistical plots of test results for 50 samples

For 50 samples, 46 met the first stage (92%), 42 met the second stage (84%), and 4 failed in both stages (8%).

Some sample test form

|  |  |  |
| --- | --- | --- |
| Test the ransomware name | Defence degree 1 | Defence degree 2 |
| LockBit1 | reach the standard | reach the standard |
| Cerber15 | reach the standard | reach the standard |
| CryptoShield\_2 | reach the standard | reach the standard |
| CryptoWire\_9 | Not up to standard | Not up to standard |
| Gandcrab\_12 | reach the standard | reach the standard |
| Maze\_11 | reach the standard | reach the standard |

|  |  |  |
| --- | --- | --- |
| Crysis14 | reach the standard | reach the standard |
| MaMoCrypter | Not up to standard | Not up to standard |
| Ransomware.FRS\_2 | reach the standard | reach the standard |
| Dharma\_10 | reach the standard | Not up to standard |

Test results analysis

In some test samples, two samples of ransomware (CryptoWire\_9 and MaMoCrypter) did not reach the level of defense 1, which can be found in common is that neither of the decoy files are operated, and CryptoWire\_9 only encrypted the desktop files. In addition, the suffix name of the two is not in the blacklist, these two points may be that the detection module can not detect them and thus unable to complete the subsequent reduction and clearing operation, but can only reach the defense degree 1. And 1 (Dharma\_10) did not reach the standard of defense degree 2, it can be detected but in the reduction clearance link, so you can speculate that the ransomware is detected module smoothly detected but after restore clear reset system, the start priority is higher than the system to ransomware clearance, the final encryption to file.