User Manual

Table of contents:

Introduction

The tLab system is a corporate local service for remote and secure analysis of suspicious objects. This system is designed to protect against new types of cyber threats against which typical antivirus software is ineffective: targeted attacks, zero-day malware, and user-targeted attacks.

tLab conducts autonomous analysis of program behavior and identification of malicious functionalities on the server (corporate cloud). The system allows for the automation of the behavior analysis procedure for any programs and detects signs of malicious functions within them.

Suspicious objects are launched in virtual containers, where continuous analysis of the behavior of all running programs is conducted.

A unique deep analysis technology of program functionality is used for reliable detection of malicious objects, including zero-day threats.

This technology has an innovative aspect, which involves a mechanism for recognizing specified malicious functionalities. It tracks the behavior history and correlates events of various processes in real time.

User Manual Authorization

To use the system, it is necessary to log in with a username and password provided by the administrator. Authorization is performed on the system's login page. To log in, enter the username and password in the respective fields. User creation is described below in the section on User Administration.

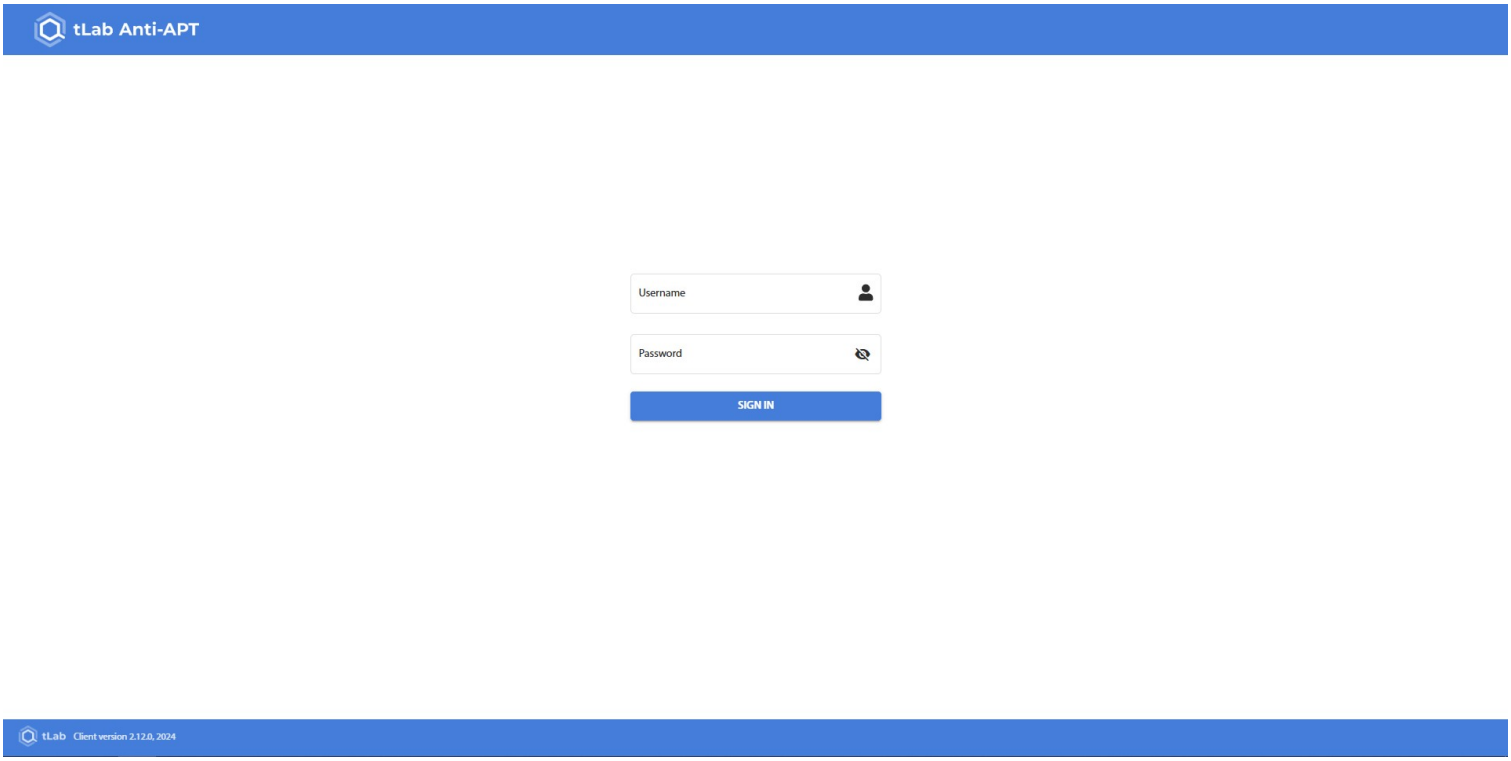
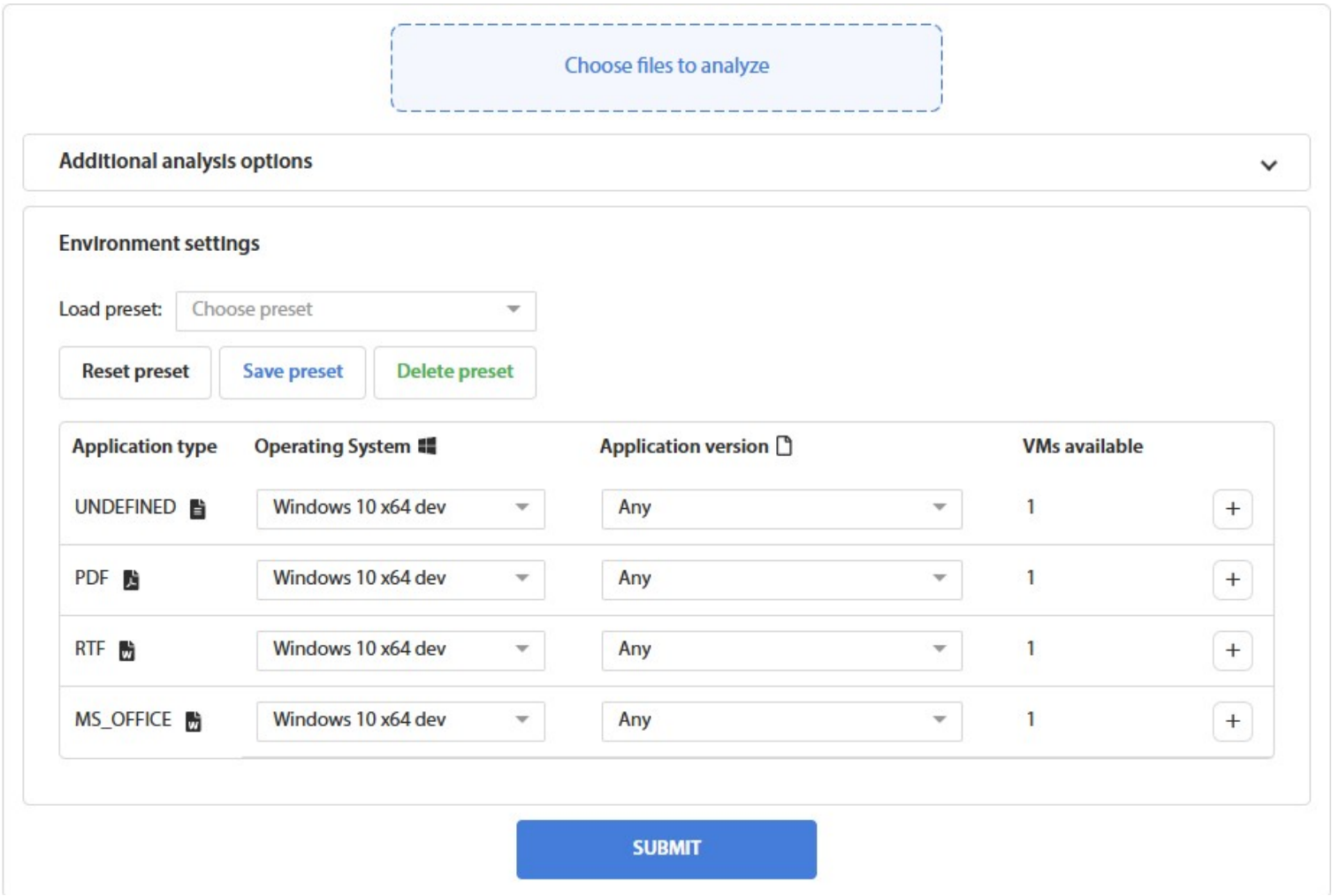


Fig. 1 – Login Page

File Upload

File uploads for checking are carried out on the File Upload tab of the Upload page, which is accessible through the top navigation menu. Clicking the 'Select Files for Checking' button will open a dialog box to choose files of any type. In the dialog box, it is possible to select a group of files either by mouse selection or by using the Ctrl + Left Mouse Button combination. In this version of tLab, uploading folders is not supported, only individual files.



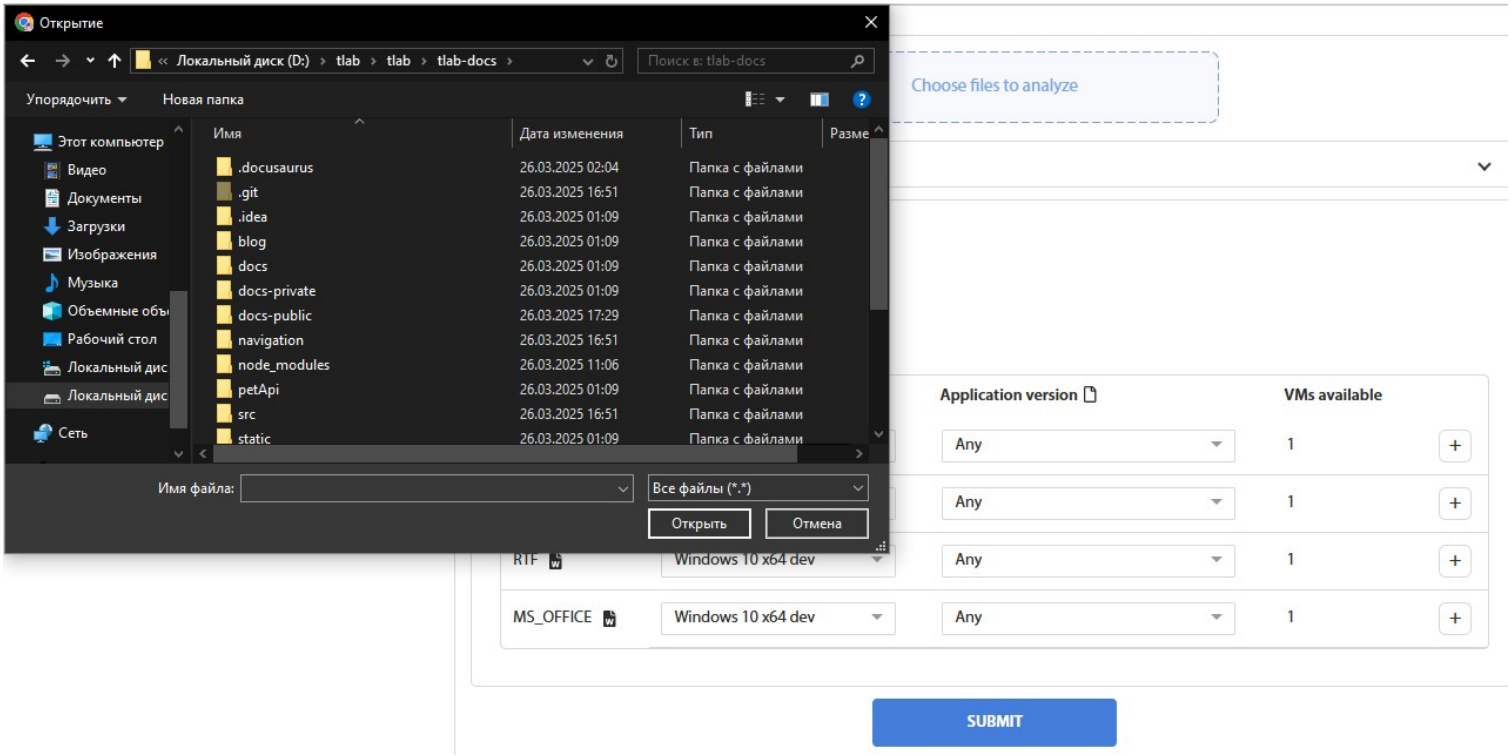


Fig. 2 — File Selection Dialog for Upload

After selecting the files, the 'Open' button will close the file selection dialog box. By repeatedly clicking 'Select Files for Checking,' you can choose files located in different directories. The default total number and size of files are limited to 10 files and 100 Megabytes, respectively.

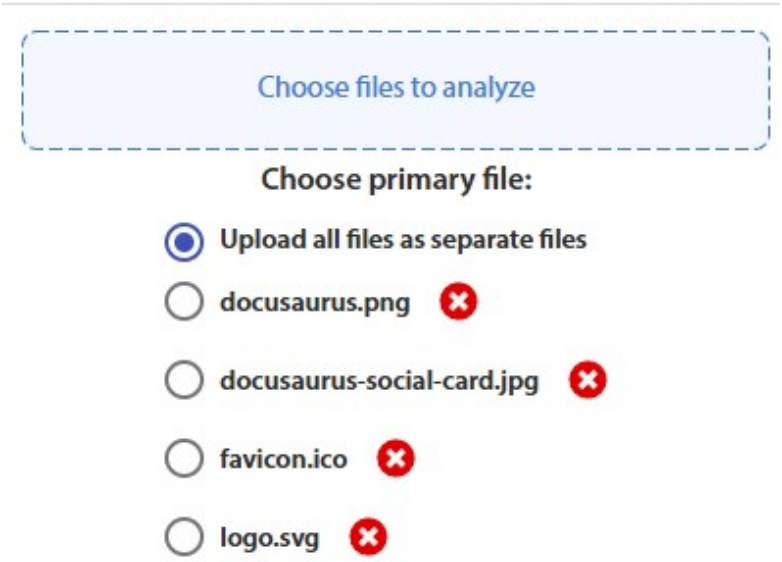


Fig. 3 – Upload Form After Selecting a Group of Files

You can cancel the selection of files (or a group of files) by clicking the red 'X' next to the file (or group).

When uploading a group of files, it is possible to perform a dynamic analysis of the entire group. This feature is necessary for checking files with dependencies. To do this, you need to select the main file, which will be

executed during the analysis. The other files will then be used as dependencies and placed in the same directory.

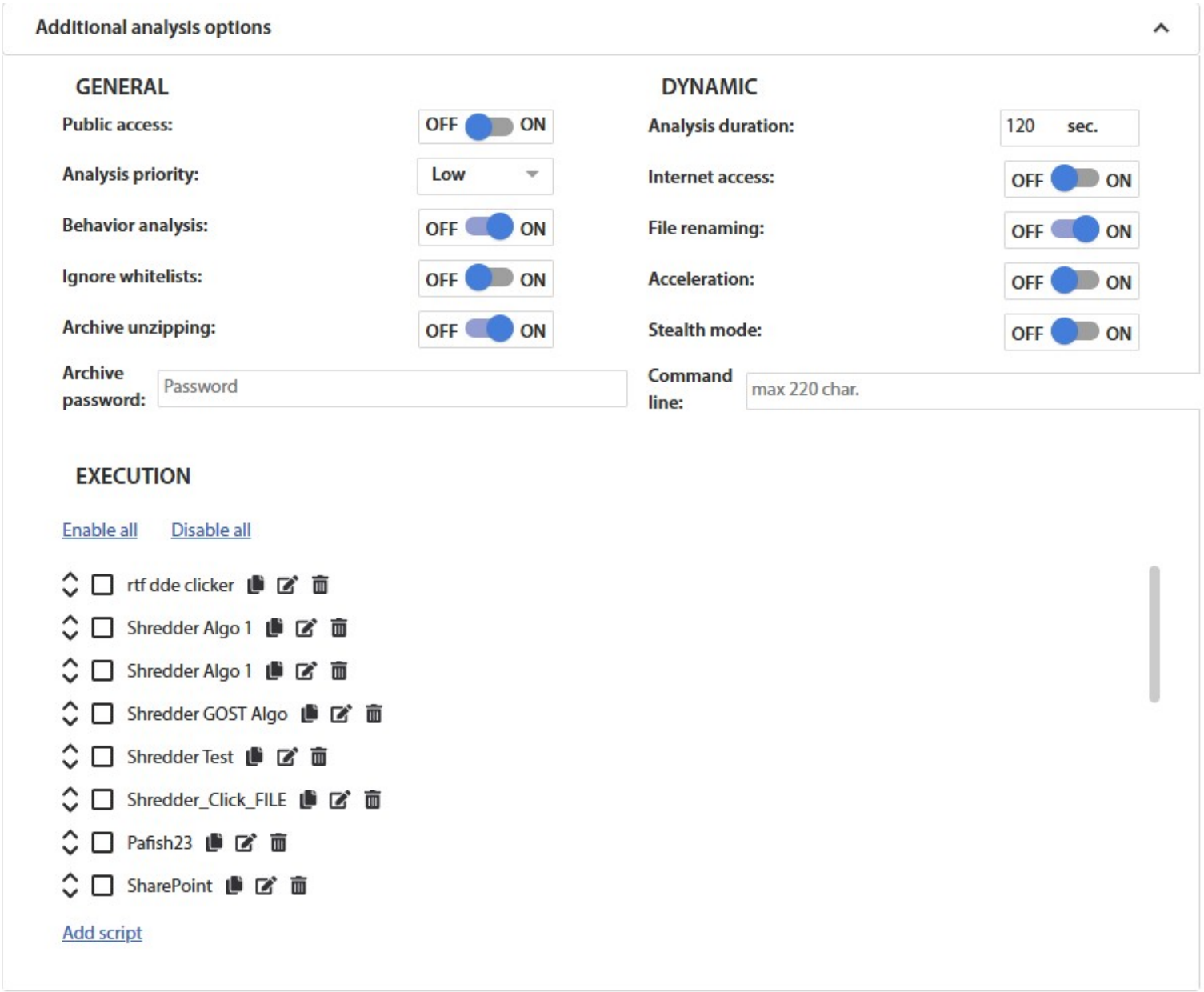


Fig. 4 – File Upload Form with Additional Settings

Additional analysis properties allow you to modify extra settings for the analysis. Here is a list of possible properties:

Public access – Enabling this option makes the reports of selected files available for viewing by all system users. Otherwise, access to the generated reports is restricted to the user who uploaded the objects and the administrator.

Analysis priority – Allows for more urgent analyses to be conducted out of turn.

Analysis type – Enables or disables the conduct of static and dynamic analyses. By default, all types of analysis are performed.

Ignore whitelists – By default, trusted files are not analyzed, and a message about their trusted status appears. When this option is enabled, all files, including those on the whitelist of trusted files, are analyzed.

Archive unzipping – Activating this option triggers the unpacking of uploaded archives and conducts a separate analysis for each object contained within the archive. Activating this option does not affect the processing of other types of files during upload.

Archive password – This field is used for entering the password for the archive, if one is required.

Analysis duration – Used to set the duration of the dynamic analysis. The default is 2 minutes, with a maximum of 60 minutes.

Internet access – Grants access to the internet from the container during dynamic analysis. Caution is required when analyzing network-spreading viruses such as WannaCry and Petya. By default, network access is disabled.

File renaming – Activating this option changes the original name of the uploaded object during dynamic analysis. This name is then used in the event chain.

Acceleration – Enabling this option mitigates the main types of delays, including hard-to-eliminate micro-delay loops.

Command line – Allows specifying command line parameters for launching the analyzed file during dynamic analysis..

Versions – This option allows the selection of the environment for dynamic analysis for Microsoft Office and Adobe Reader documents. Choosing more than one version will create multiple analyses and generate several reports.

For one analysis, it is advisable to select an environment from one group (for example, only from the Microsoft Office or Adobe Reader group).

User Activity Simulation Scenarios – On this panel, scenarios used during the dynamic analysis of an object with a graphical interface are selected. Each scenario has a name, activation conditions (matching by window title and/or process name), commands to be executed, minimum and maximum number of command repetitions, delay before performing actions, and delay between actions. Scenarios are executed in order from top to bottom, allowing for the creation and sequential execution of multiple scenarios for specific

programs, for example, Scenario #1 presses the TAB button three times, while Scenario #2 presses the ENTER button.

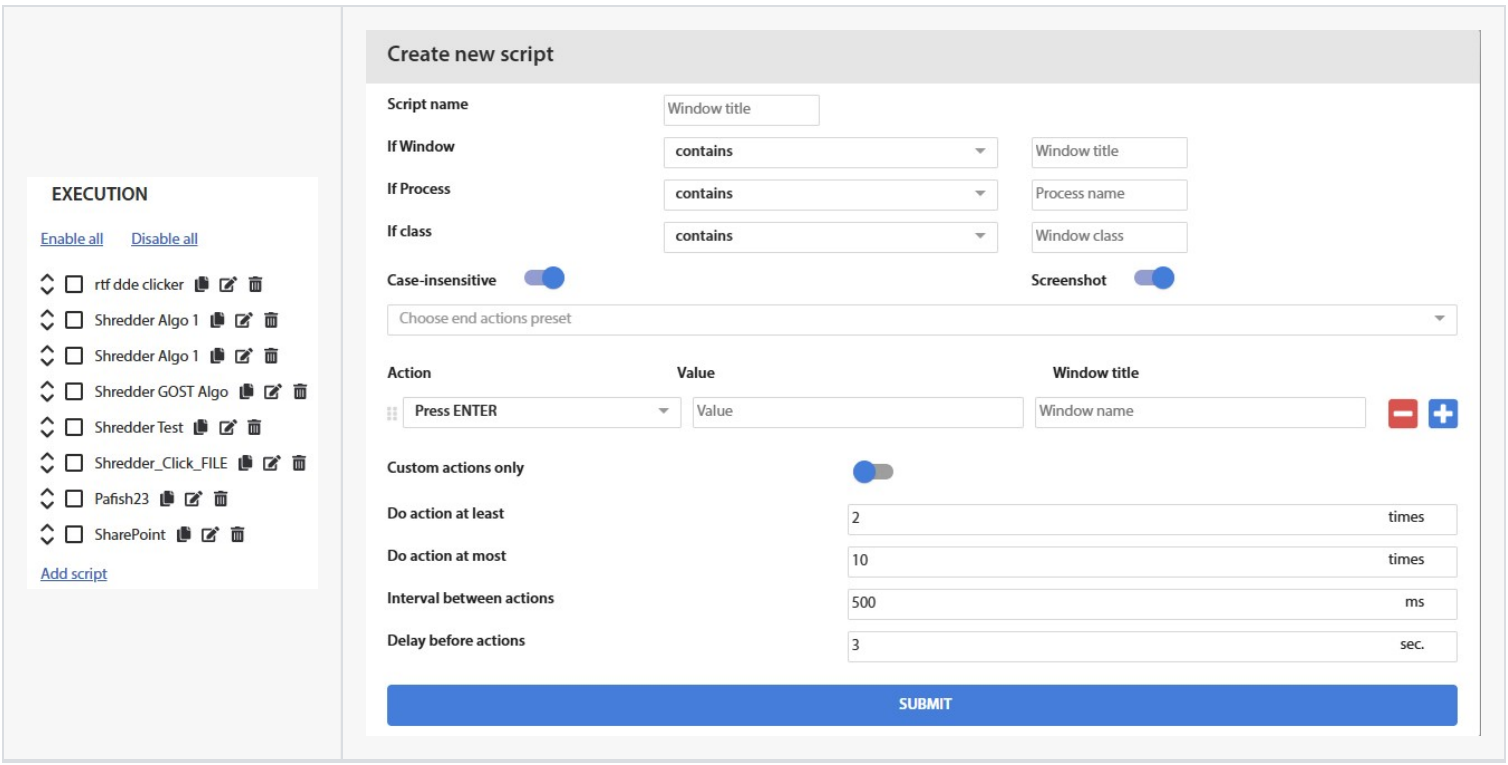


Fig. 5 – User Activity Simulation Scenarios

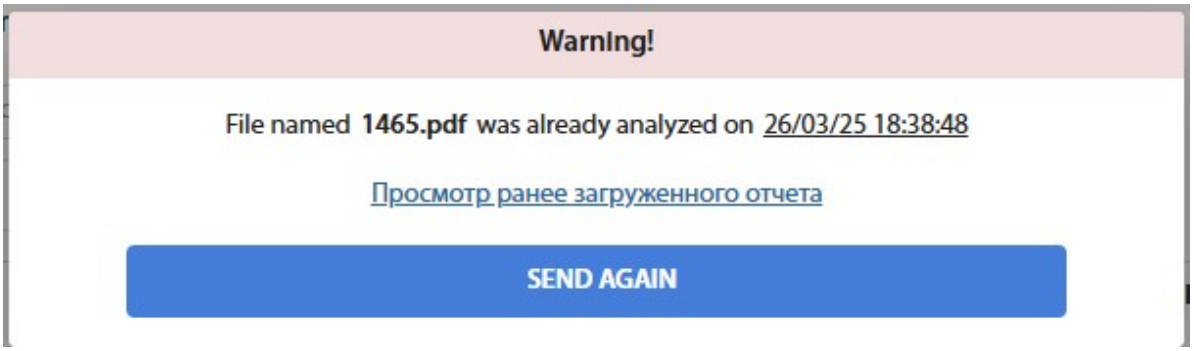


Fig. 6 – Duplicate Upload Message

When re-uploading a file that already exists in the tLab system, a message will appear with an administrative note, a link-date to the latest report, and a 'Resend' button for reanalyzing the file.

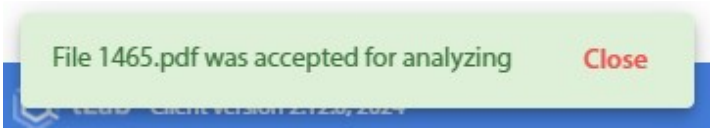


Fig. 7 — File Upload Success Message

Analysis Queue

Uploaded files for analysis are placed in the verification queue. Clicking the **Queue** button in the top navigation panel of the web client opens a page displaying the list of queued objects. If there are files in the queue, a number indicating the count of queued elements is displayed to the right of the **Queue** button. Analyses with a higher priority are positioned above lower-priority analyses in the queue, and their reports are generated earlier. The queue page updates automatically, and completed analyses are removed from the queue.

The **Failed Analyses** tab displays a list of analyses that ended with an error. For each file, the error type and a list of all failed attempts with that file are shown. Once a previously failed file is successfully analyzed, its entry will be removed from the **Failed Analyses** list.

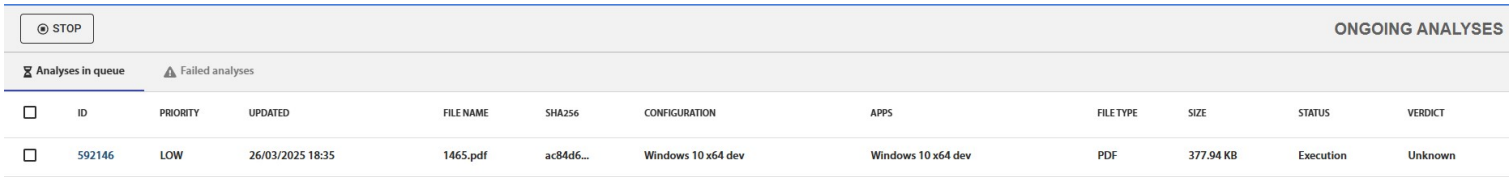


Fig. 8 – Analysis Queue

Reports

The table with completed reports can be displayed by clicking the **Reports** button in the top navigation menu. The number displayed to the right of the **Reports** button indicates the count of unread reports.

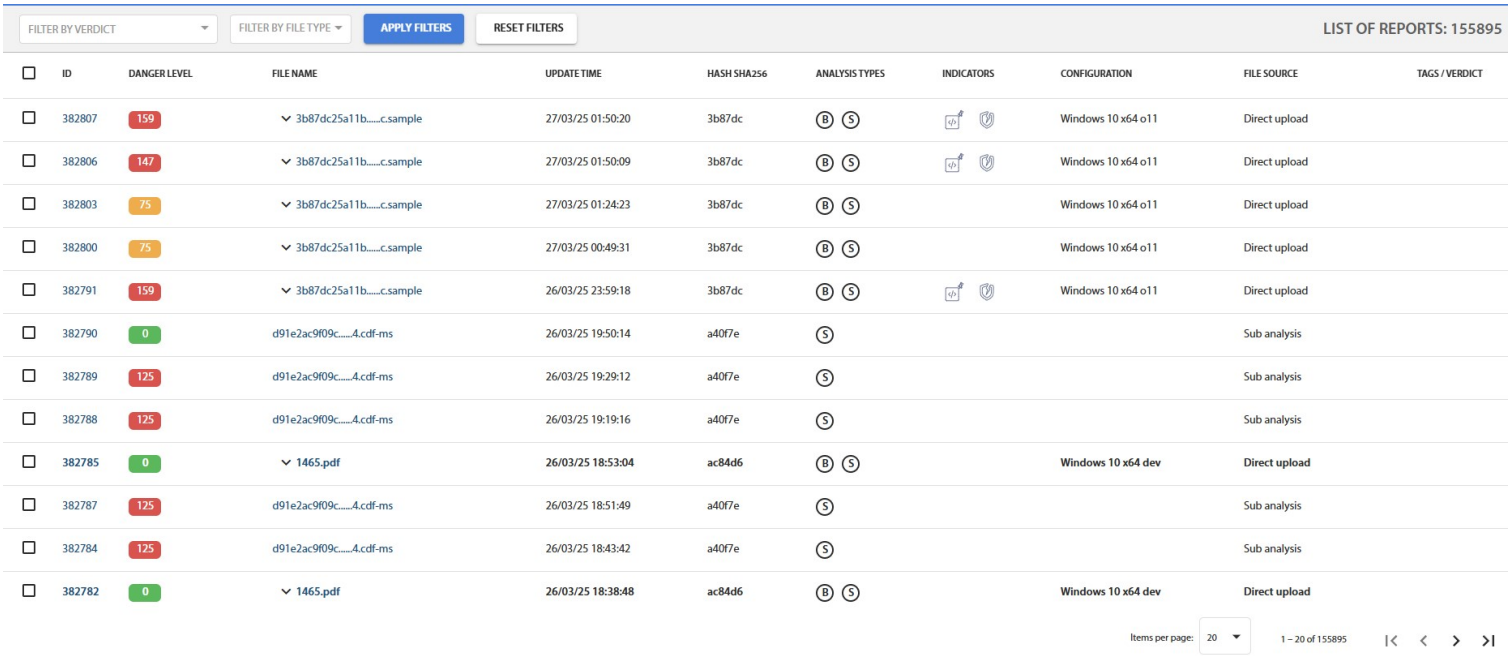


Fig. 9 – List of Generated Reports

The table contains the following columns:
Checkbox for selecting multiple reports to perform operations on a group of objects;

- Report read status;
- Analysis type (a set of icons) – dynamic, static;
    - Ⓓ - Dynamic analysis execution status
    - Ⓓ - Dynamic analysis completed
    - Ⓢ - Static analysis completed.
- Report generation date and time;
- File name – a link to the report and the name under which the file was uploaded;
- SHA256 hash value of the file, which can be used for quick search of identical files.;

- File activity indicators (a set of icons), such as internet activity, process injection, service creation, autostart execution (a list of possible indicators is provided in Appendix 1);
- Number of screenshots taken during dynamic analysis.
- Threat level calculated by the tLab system based on the volume and maliciousness of activities detected during dynamic analysis. The higher the value, the more dangerous the file;
- Danger indicator shows the file's risk level on a color scale: green – safe, orange – requires attention, red – high likelihood of maliciousness;
- Expert or administrator conclusion. The conclusion is provided within the report.

Clicking the Filters button displays an additional menu where you can sort the list of reports by various properties or select the number of results displayed per page. The Select All button highlights all reports on the page, allowing actions to be performed on them: Mark as Read/Unread or Delete. Deleted files are moved to the trash, which is accessible only to the administrator. Accidentally deleted files can be restored from the trash.

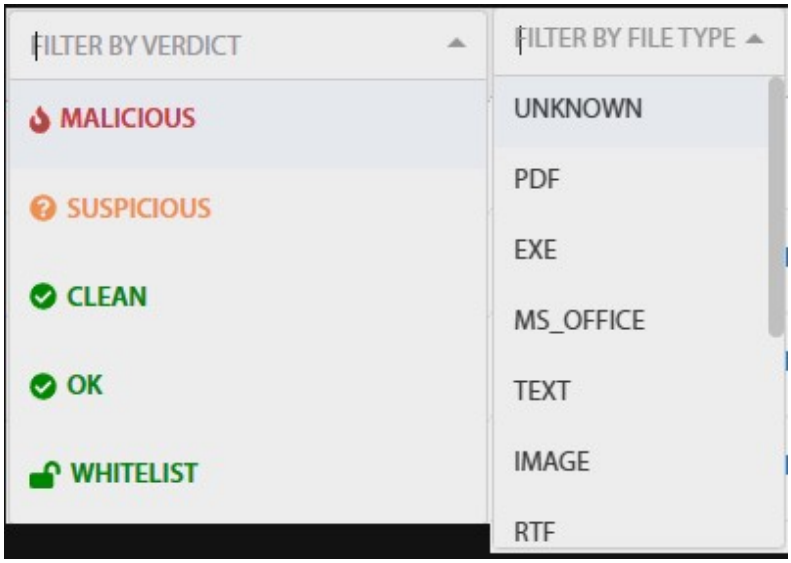


Fig. 10 – Filter Menu

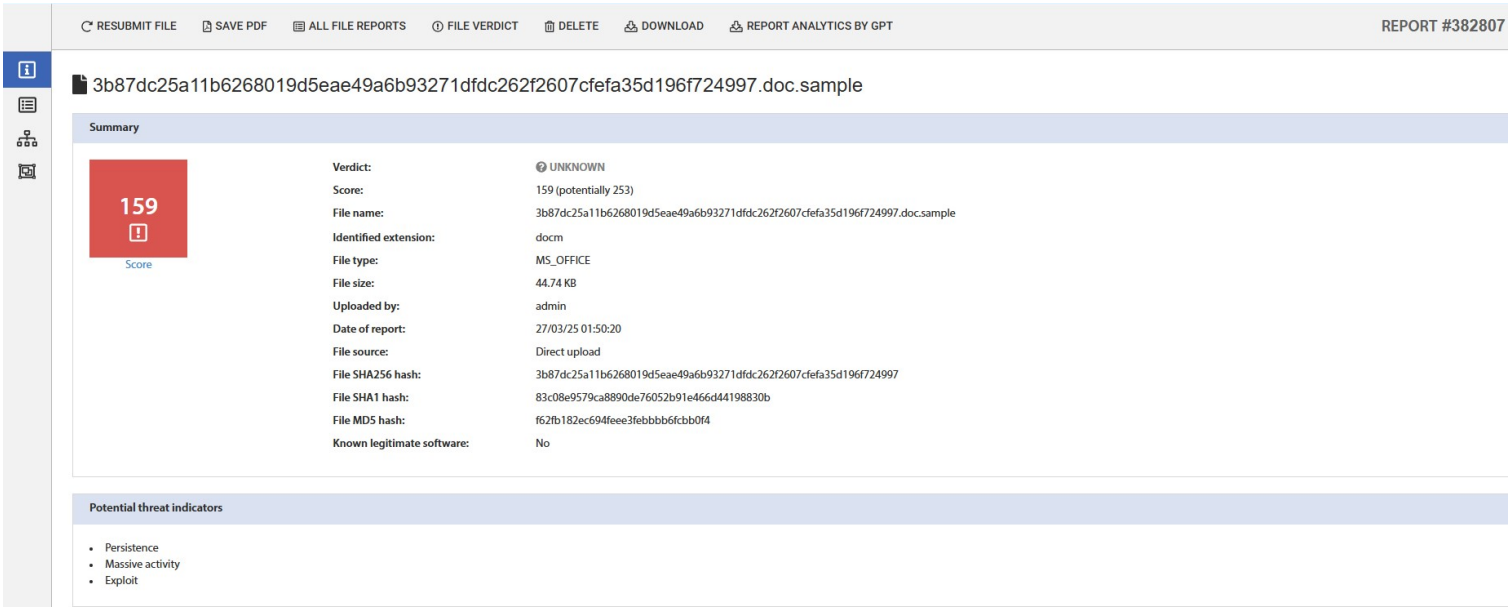


Fig. 11 – General Report

The report page consists of three vertical tabs. The General Report tab contains general information about the file, the expert's conclusion, and analysis parameters. The Static Report tab includes data collected by the static analyzer. The Dynamic Report tab presents the results of the dynamic analysis. Clicking the File Operations button displays the corresponding menu:

- Resend (opens the form for resubmitting the file for analysis);
- History (a list of all reports for this file with date-links to the reports);

Fig. 12 – File Operations Menu

Clicking the **Search button** in the navigation menu opens the report search page in the system. The search is conducted across multiple fields, which can be found in the general report and are also displayed in the corresponding columns of the report list and queue. When entering 4 to 6 characters in the SHA256 search field, a dropdown list appears showing reports that contain matching characters. To access the found report, the full hash value must be entered (or selected from the list) and the **Search** button pressed.

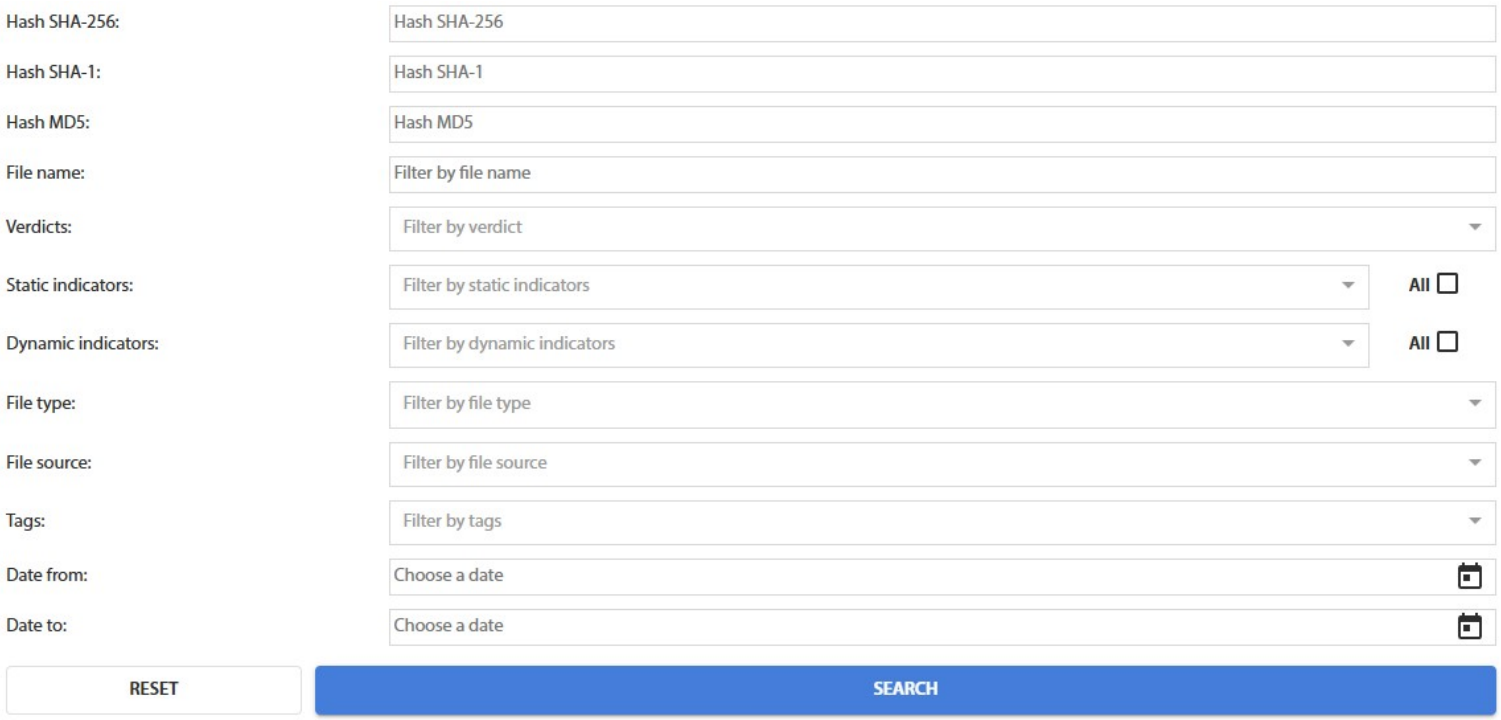


Fig. 13 – Report Search Page

Static Analysis Report

The static analysis page displays the results of analyzing the file's static information, meaning the examination of the file's contents without executing it.

In the tLab system, the threat level of static analysis is calculated based on static threat indicators, such as the import of suspicious API functions, the presence of scripts and macros in documents, anomalous section structures, encrypted data, low-level operations capability, embedded files, and more.

The static analysis report contains specific information depending on the file type.

For PE executable files:

- A collapsible list of imported modules and functions;
- A list of exported functions;
- A list of extracted strings with partial match search functionality;
- Program icon;
- Information about executable file sections.
  For MS Office and PDF files: document metadata such as author, number of pages, title, year, etc.
  For script analysis:
  - Possible activity;
  - Detected activity;

  For Android application analysis:
  - Application information;
  - Android analysis;

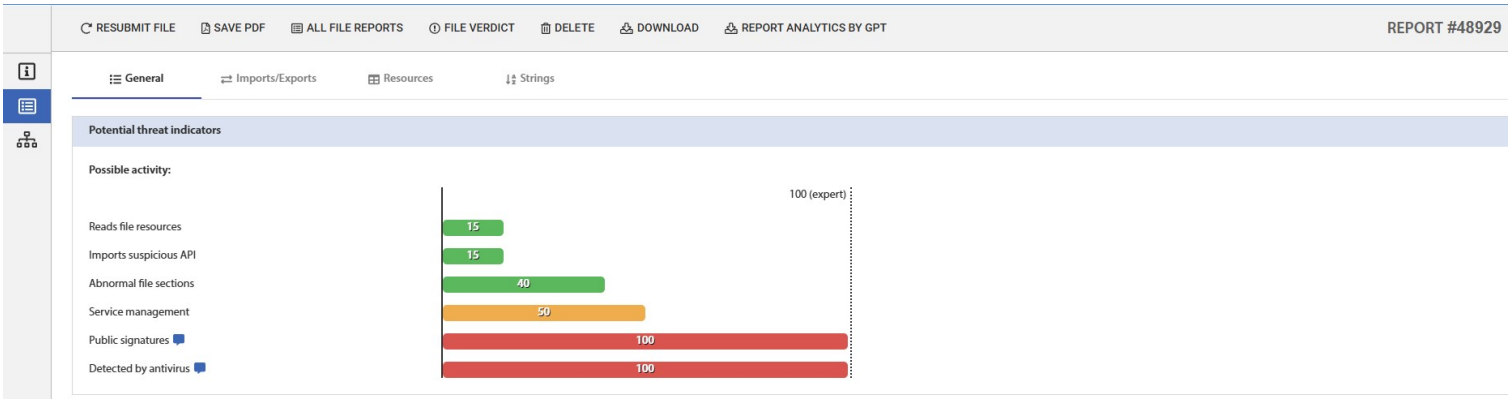


Fig. 14 – Static Analysis Report

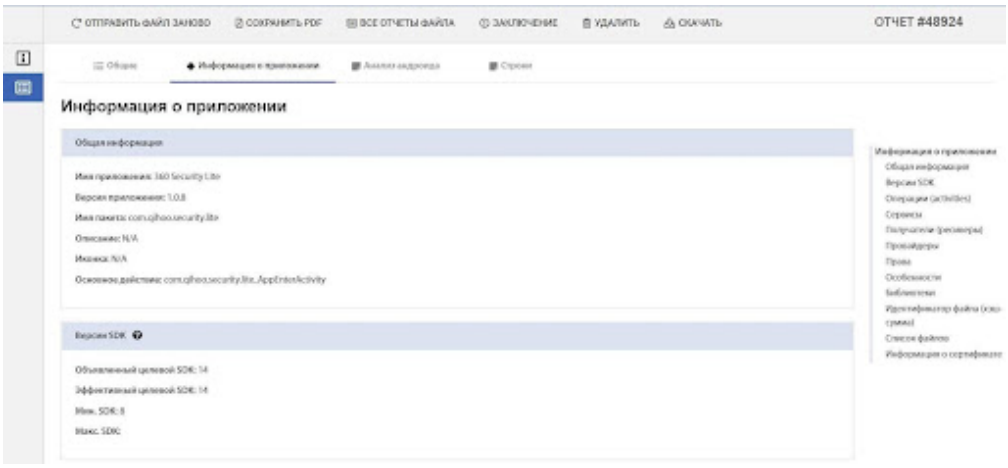


Fig. 14.1 – Android Application Analysis Report

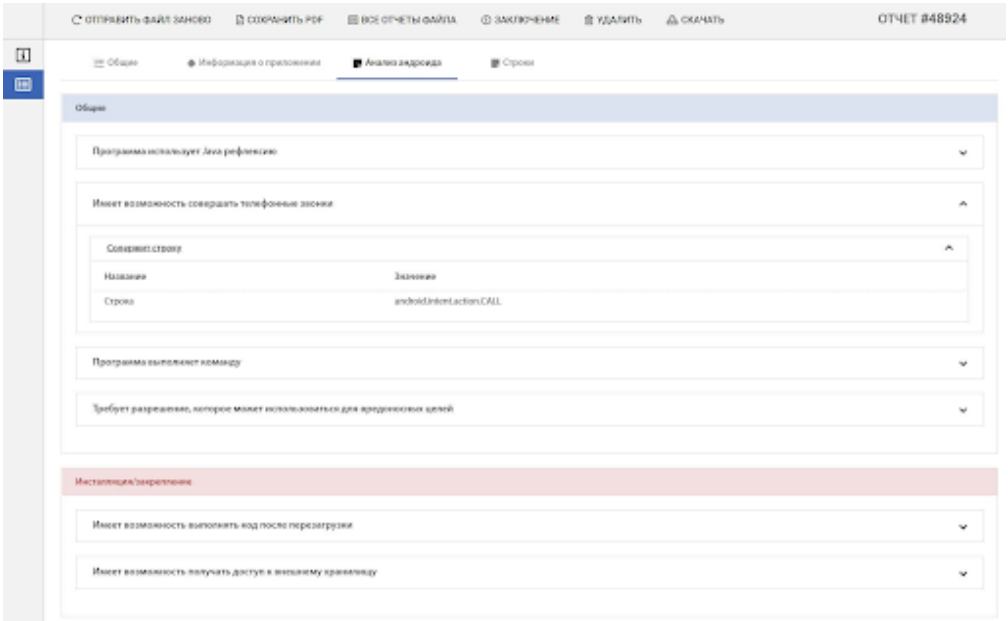


Fig. 14.2 – Android Application Analysis Report

DeepSlicer

DeepSlicer is a static analyzer. It reads the script text, determines the language in which it is written, and provides information about its suspicious functionality without direct execution, such as registry modifications or file download.

In Fig. 14.3.1, potential activity is shown – functions that are present in the code but may not be executed.

In Fig. 14.3.2, detected activity is shown – functions that are explicitly called in the code.

> **WARNING**
> Pay attention to potentially malicious activity.

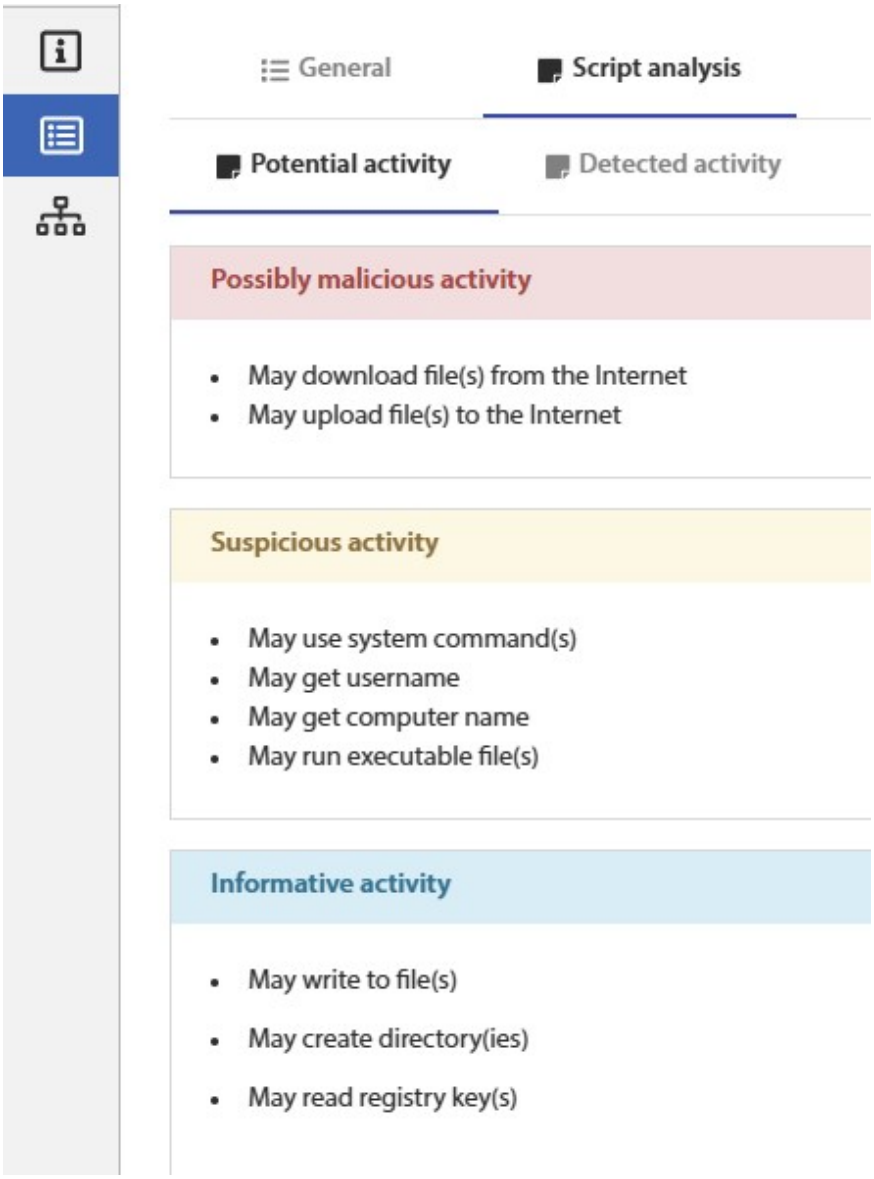


Fig. 14.3.1 – DeepSlicer Page: Potential Activity

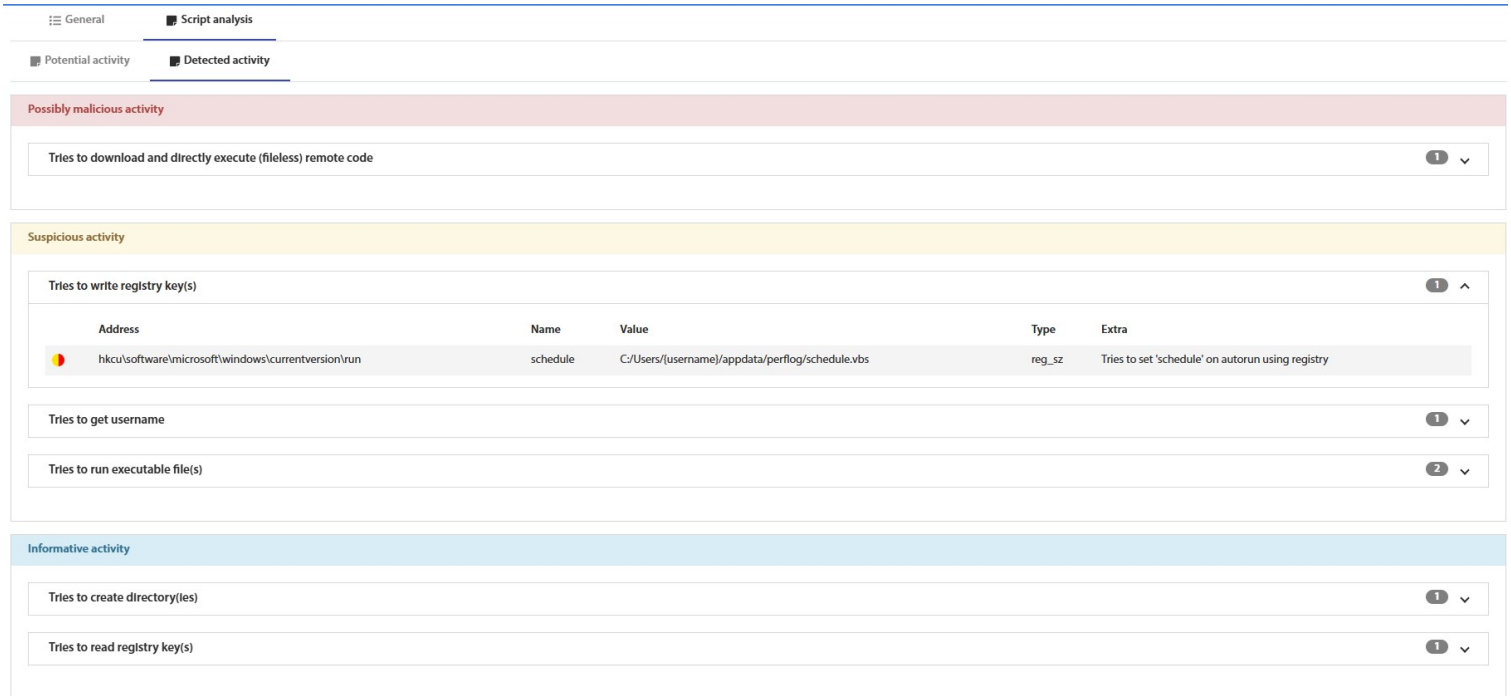


Fig. 14.3.2 – DeepSlicer Page: Detected Activity

Fig. 14.3.3 – DeepSlicer Page: Legitimate Activity

Structural Validation Binary Eye

It allows describing file structures in a convenient and fast format. Using programs written in this language, instructions for validating files and objects can be compiled. This approach enables the rapid implementation of static analysis for various file formats and vulnerabilities.

The module analyzes files for compliance with a specific specification by automatically parsing and examining the document structure, highlighting individual sub-objects and fields.

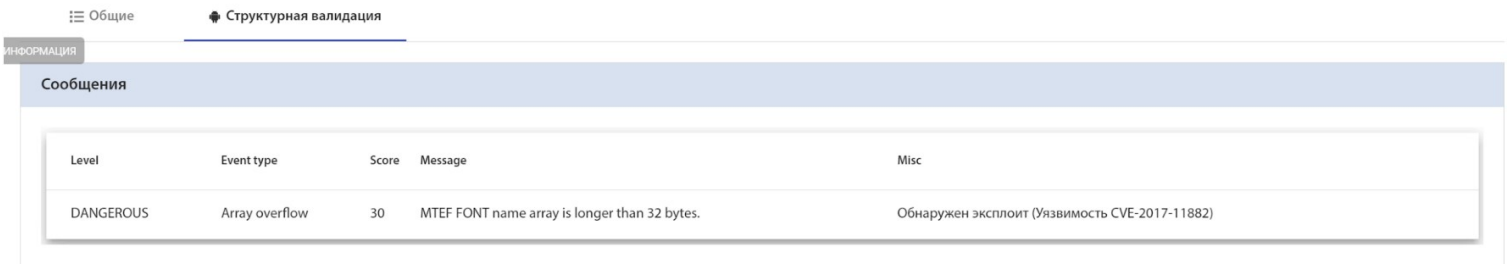


Fig. 14.3.4 – Structural Validation Page

Dynamic Analysis Report

The dynamic analysis page displays the results of the dynamic analysis conducted on a virtual machine within the execution environment.

The summary report displays indicators of potential threats and a collapsible list of detected activities.

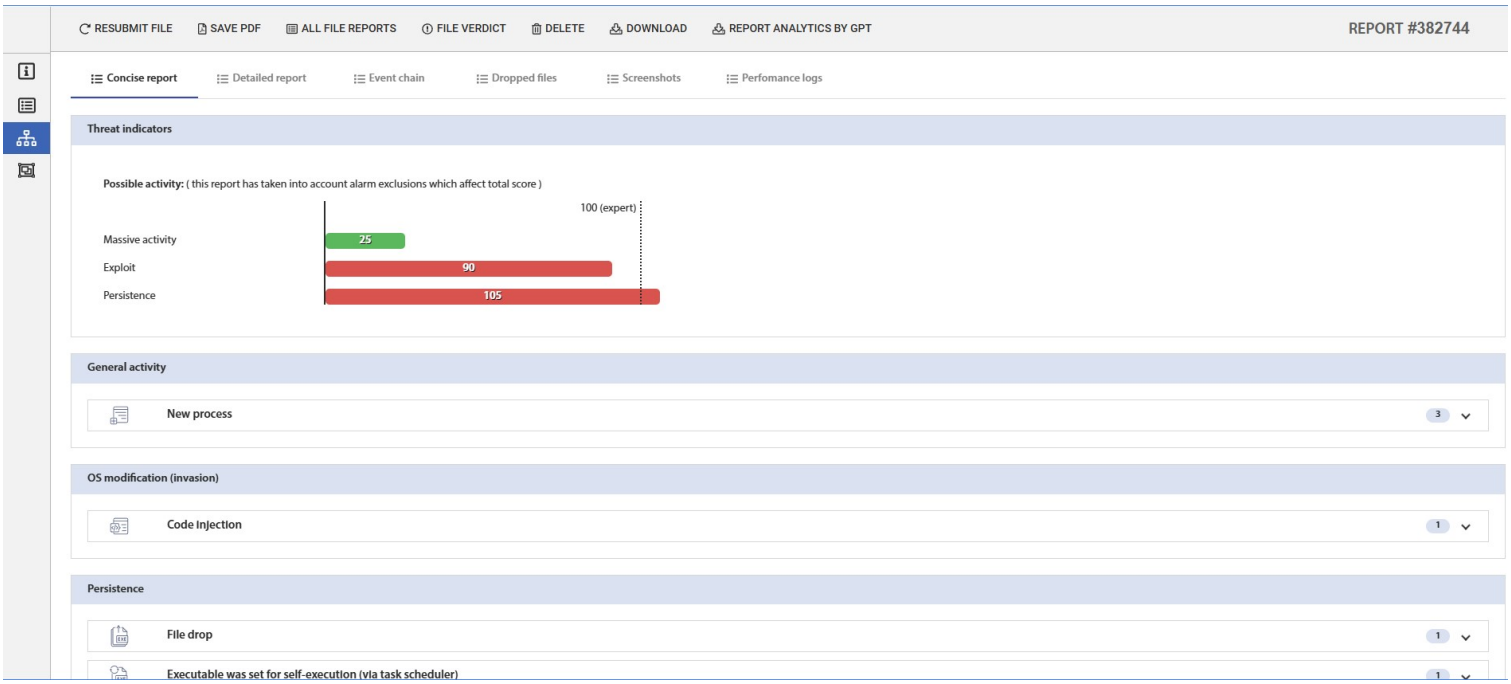


Fig. 15 – Dynamic Analysis Report

Detailed Report

The detailed report is an interactive list of activities with filtering options by event type. A full list of activities with their parameters is provided in Appendix 2. Right-clicking on an activity parameter opens a context menu with additional filters for that parameter. Each activity has a danger level, with possible danger levels listed in Appendix 3.

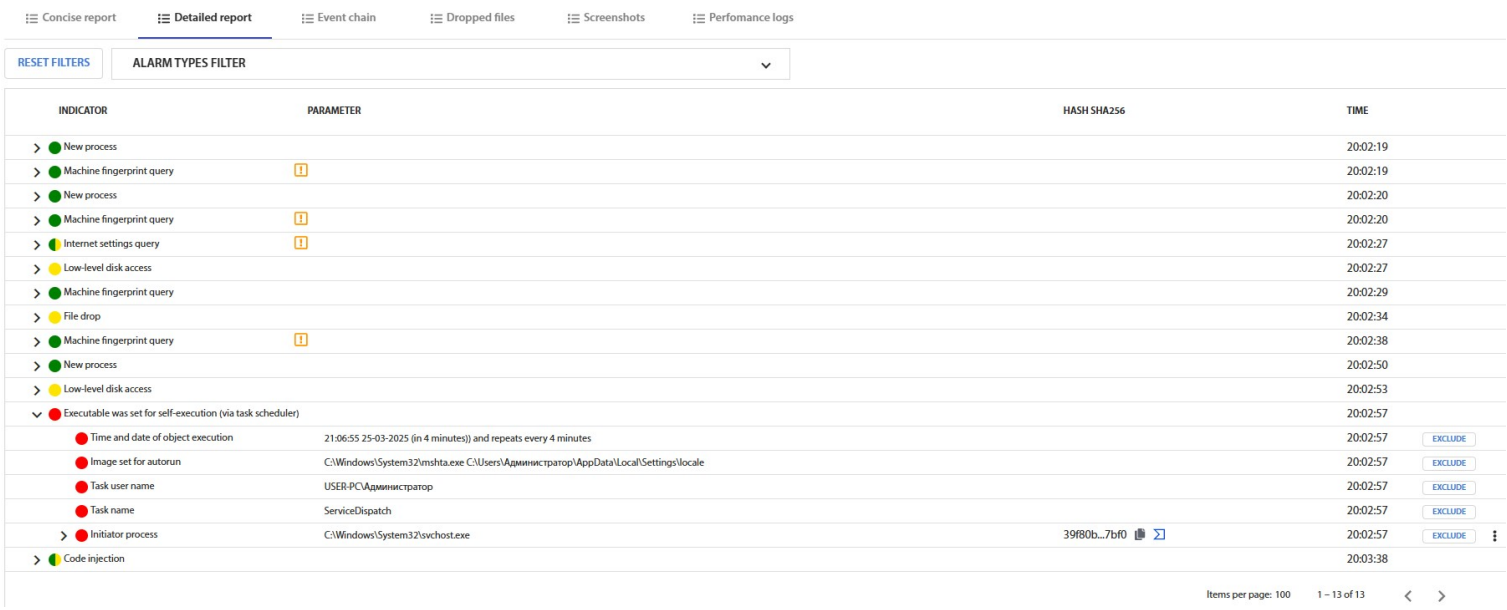


Fig. 16 – List of Recorded Activities

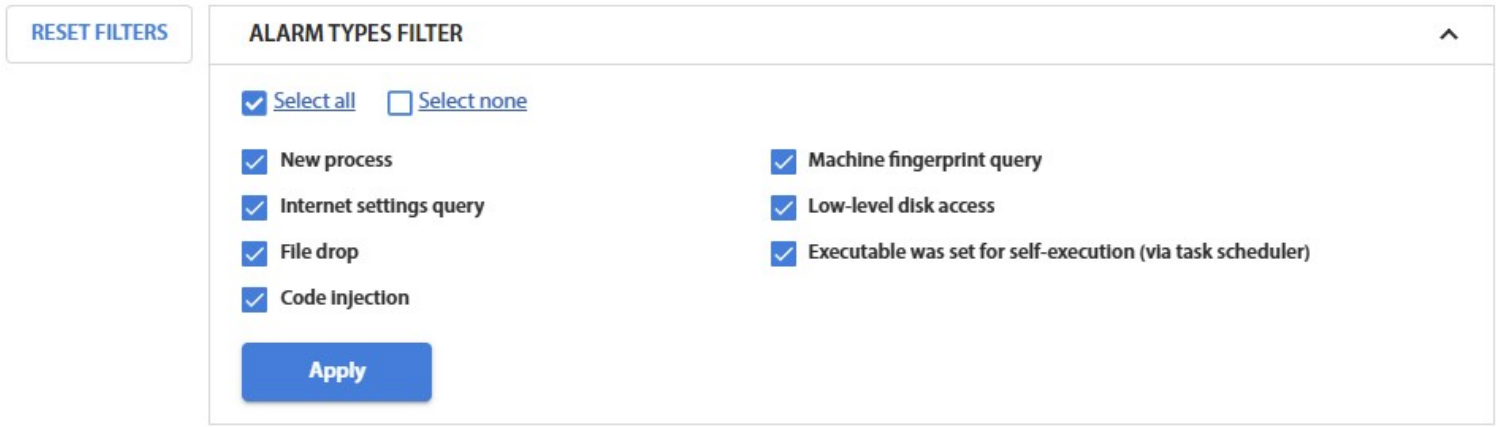


Fig. 17 – Filters for the List of Recorded Activities

Fig. 18 – Filters for the List of Recorded Activities, Available via the Context Menu

The system provides the ability to add a file or path to the exclusion list for analysis. By selecting a path or part of it and right-clicking, a menu will open, allowing access to the exclusion addition window.

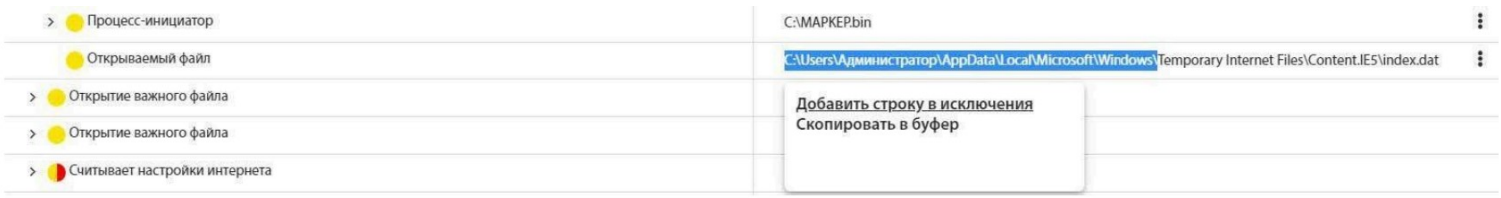


Fig. 18.1 – Defining the File/Directory Exclusion Path

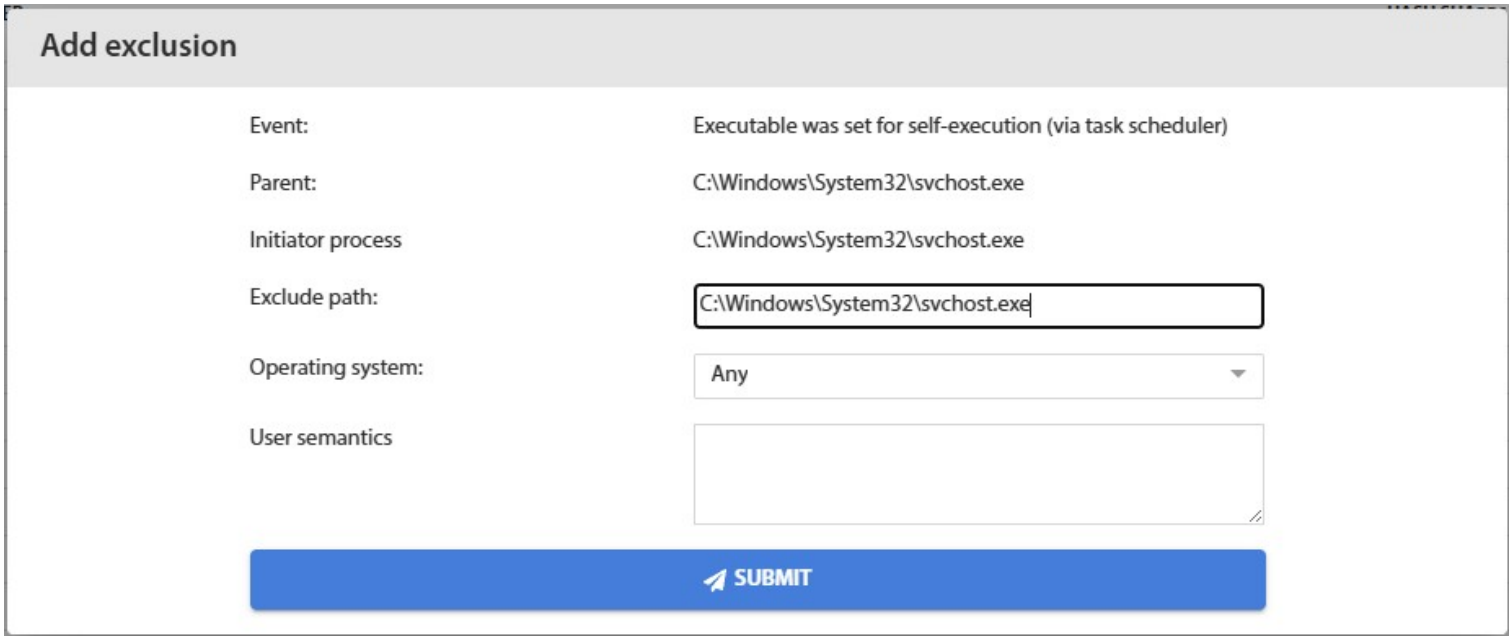


Fig. 18.2 – Exclusion Addition Window

Event Chain

The event chain is an interactive event tree. The maximum tree size before display is limited by the number of visible elements.

The full-screen mode opens a pop-up window for more convenient viewing of large trees. The mouse wheel can be used to zoom in and out of the tree. Left-clicking and dragging allows adjusting the viewing area. Clicking on an event highlights all events in the tree with similar paths in red. The **Highlight in Different Colors** option reveals previously hidden tree elements and assigns the same color to events with similar paths. A list of activity tree events is provided in Appendix 4.

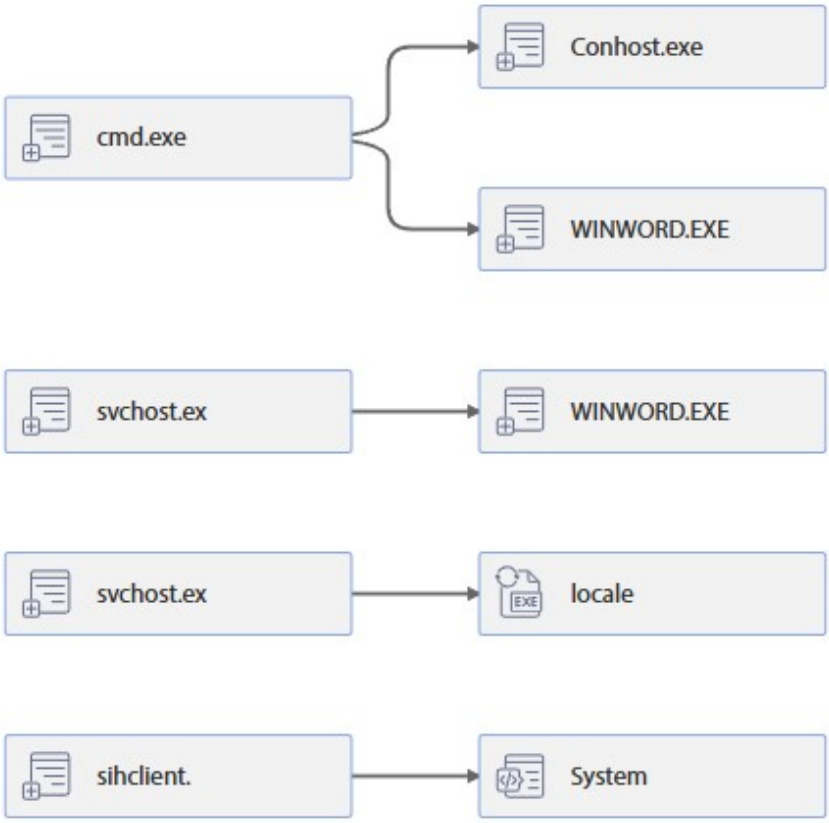


Fig. 19 – Activity Representation as an Event Chain

Screenshots

Screenshots – a gallery of screenshots taken when a graphical user interface is detected in the analyzed files. Green highlights indicate areas where changes were detected between two consecutive screenshots. Disabling the Highlight Changes option hides such screenshots. Screenshots displaying a mouse cursor indicate left-click actions during the simulation of user activity on a specific interface element that triggered a change on the screen. A timestamp in the format `<minutes>:<seconds>.<hundredths of a second>` from the start of the analysis is displayed in the bottom right corner of each screenshot.

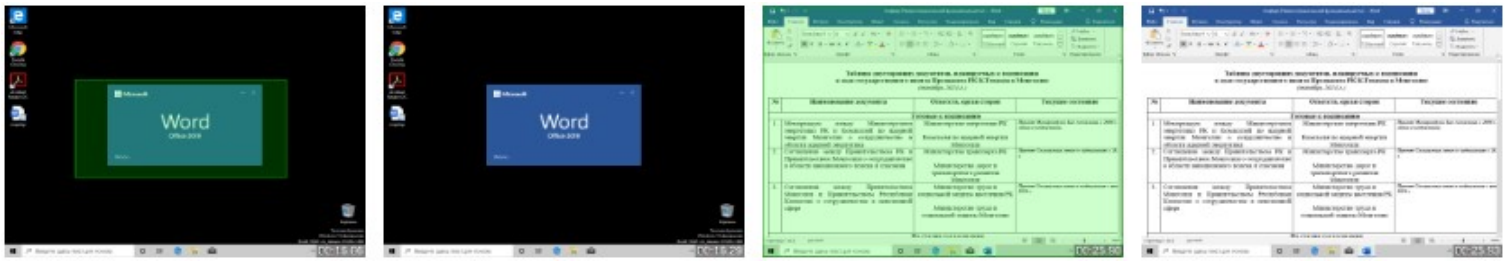


Fig. 20 – Screenshot Gallery

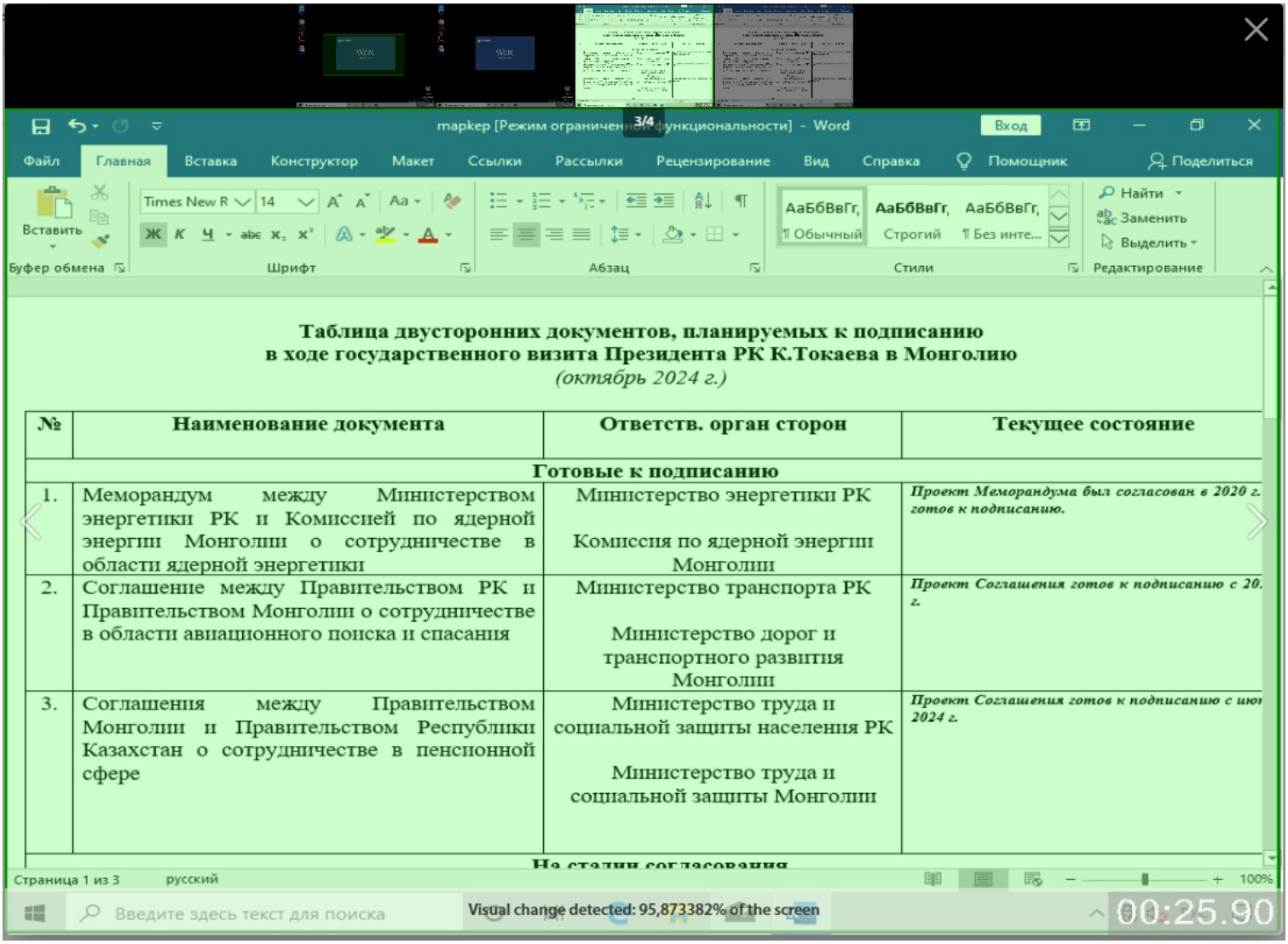


Fig. 21 – Screenshot

Network Analysis

This page displays information about the network analysis of the PCAP file.

> **WARNING**
> This analysis is performed only if internet access was enabled during file analysis.

The network analysis includes information on DNS requests, HTTP traffic, and interactions with hosts.

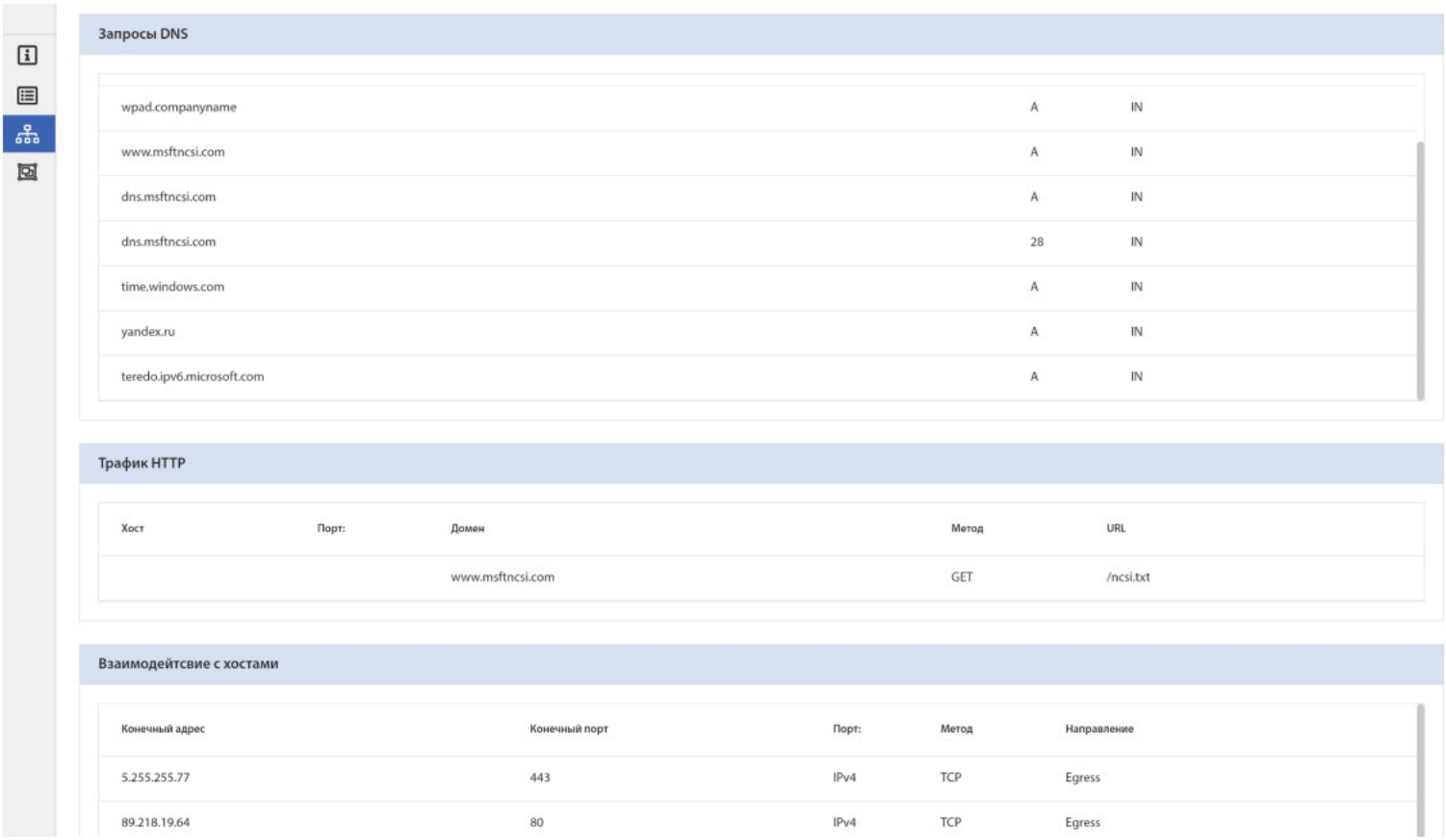


Fig. 21.1 – Network Analysis Page

Dropped Files

This page displays information about files dropped during dynamic analysis. This means that if, during dynamic analysis, processes drop additional files, they are sent for separate analysis. Information about these files is shown on this page.

Dropped files are listed in the report table and can be found using their hash values.

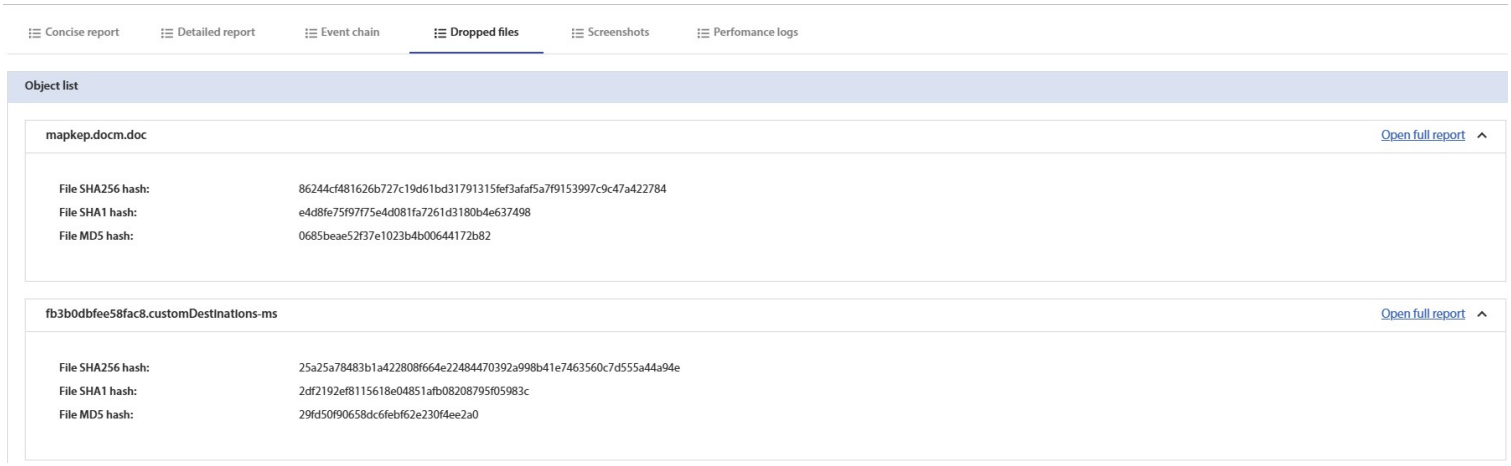


Fig. 21.2 – Dropped Files Page

Performance Logs

This page displays graphs of CPU and memory usage by various processes detected during the dynamic analysis of the file.

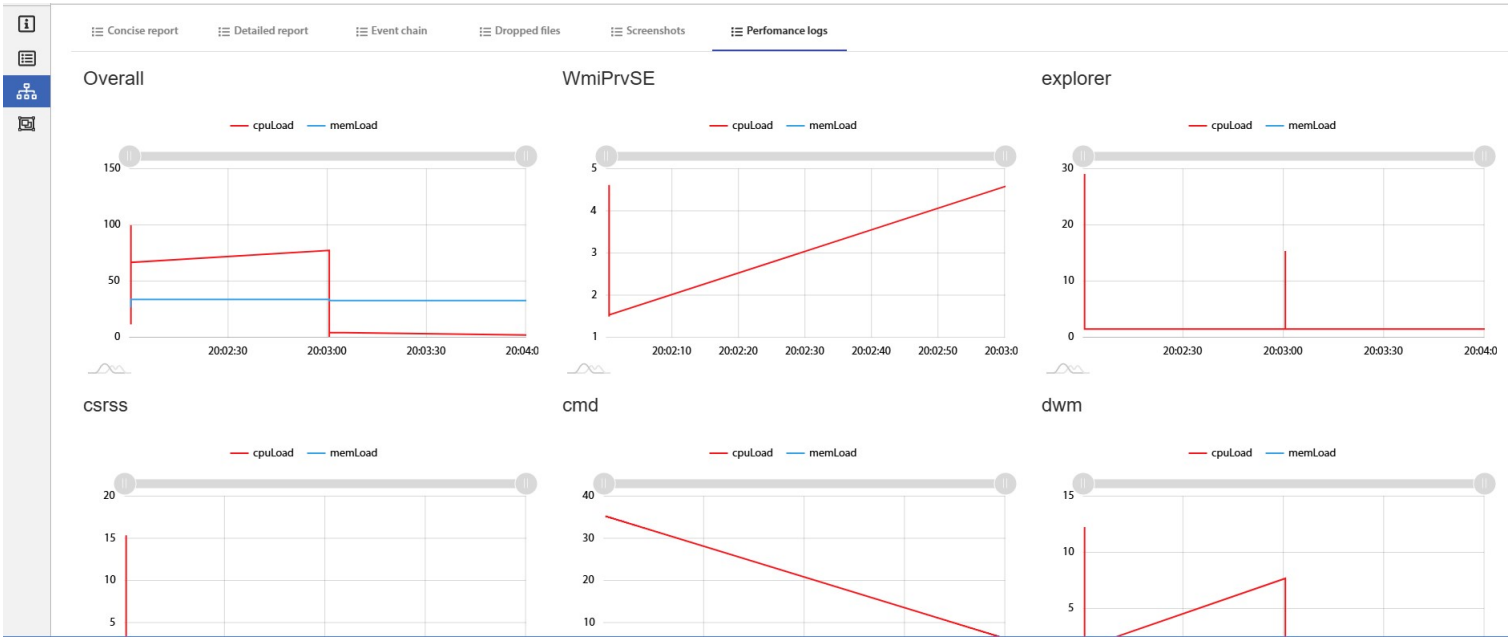


Fig. 21.3 – Performance Logs Page

Appendix 1 – Activity Indicators

 - Persistence

 - Exploit

 - Proxy Activity (Intrusion)

 - OS Modification

 - Network Activity

 - Untrusted Process Delays Execution (Possibly to Evade Detection)

Appendix 2 – List of Activities (Events)

Event Name	Activity Parameters
Autostart	Registry Section
	Key Name
	Path to Executable Program
	Autostart Initiator Process
New Process	New Process File
	Command Line
	Parent Process
New Service	Service Name
	Path to Service Program
	Initiator Process
Code Injection	Target Process for Injection
	Initiator Process (Injector)
Keylogger	Spy Process
	Victim Program
	Keystroke Log File (Credential File)

Event Name	Activity Parameters
Code Injection Access	Opened Process
	Source Process
Access to Autostart Registry	Initiator Process
	Registry Key Name
Executable File Extraction	File Creator Process (Dropper)
	Created File
Internet Connection Established	Connection Initiator Process
	Remote Address
	Remote Port
	Local Port
	Protocol Type
Waiting for Incoming Connection	Initiator Process Waiting for Connection
	Local Port
	Protocol Type
Internet Connection Attempt (Failed)	Connection Initiator Process
	Remote Address
	Remote Port
	Local Port

Event Name	Activity Parameters
	Protocol Type
Moving an Important File	Important File Initiator Process
	New File Name
	Old File Name
Opening Another Executable File	Initiator Process
	Opened File
Opening Multiple Executable Files	Initiator Process
	Number of Files
	File Types
	Directories
Writing to Another Executable File (Modification)	Initiator Process
	Modified File
Writing to Multiple Executable Files (Mass Modification)	Initiator Process
	Number of Files
	File Types
	Directories
Infecting Another Executable File (Code Injection into File)	Initiator Process
	Infected File

Event Name	Activity Parameters
Infecting Multiple Executable Files (Mass Code Injection into Files)	Initiator Process
	Number of Files
	File Types
	Directories
Creating a New System Task for Task Scheduler	Initiator Process
	Task Name in Scheduler
Setting an Executable File for Autostart (via Task Scheduler)	Initiator Process
	Object Set for Autostart
	Task Name in Scheduler
	Execution Date and Time
	Username for the Task
Suspicious Process Invaded a Legitimate Process (DLL Injection)	Target Process for Injection
	Initiator Process (Injector)
	Injected DLL File
Untrusted Process Delays Execution (Possibly to Evade Detection)	Initiator Process
	Execution Delay Time
	Delay Method
	System Object Name Used for Delay

Event Name	Activity Parameters
Low-Level Disk Access	Initiator Process
	Access Type
	Disk Name
Low-Level Access to Multiple Disks	Initiator Process
	Access Type
	Disk Types
	Number of Disks
Low-Level Disk Management	Initiator Process
	Disk Name
	Disk Operation Type
	Driver Control Code
Registry Key Monitoring	Initiator Process
	Registry Key Name
	Event Filter Value
	Registry Key Operation Type
Windows Installation Identification	Initiator Process
	Registry Key Name
	Windows Attribute Used for Identification

Event Name	Activity Parameters
Unique Computer Identification	Initiator Process
	Registry Key Name
	Computer Attribute (Used for Identification)
Reads Internet Settings	Initiator Process
	Registry Key Name
	Setting
Attempts to Establish Multiple Internet Connections (IP Address Scanning)	Connection Initiator Process
	Number of Network Connections
	Remote Address Subnet
	List of Remote Ports
	List of Local Ports
	Protocol Types
Low-Level Disk Write	Initiator Process
	Disk Name
	Write Start Position (Offset)
	Number of Bytes Written
	Written Text (Characters)
	Written Raw Buffer (Bytes)

Appendix 3 – Activity Danger Level Grading

- 🟢 - Normal Activity
- 🟢🟡 - Unusual Activity
- 🟡 - Suspicious Activity
- 🟡🔴 - Highly Suspicious Activity
- 🔴 - Malicious Activity
- 🔴🟤 - Critically Malicious Activity
- 🟤 - Dangerous-Destructive Activity

Appendix 4 – Activity Designations in the Event Chain

 - New Process

 - Autostart

 - New Service

 - Code Injection

 - Keyboard Access

 - Code Injection Access

 - Access to Autostart Registry

 - Extraction of Executable File

 - Internet Connection Established

 - Waiting for Incoming Connection

 - Local Network Connection

 - Internet Connection Attempt (Failed)

 - Moving an Important File

 - Opening Another Executable File

 - Writing to Another Executable File (Modification)

 - Infecting Another Executable File (Code Injection into File)

 - Opening Multiple Executable Files

 - Writing to Multiple Executable Files (Mass Modification)

 - Infecting Multiple Executable Files (Mass Code Injection into Files)

 - Creating a New System Task for Task Scheduler

 - Setting an Executable File for Autostart (via Task Scheduler)

 - Suspicious Process Invaded a LEGITIMATE Process (DLL Injection)

 - Untrusted Process Delays Execution (Possibly to Evade Detection)

 - Low-Level Disk Access

 - Low-Level Access to Multiple Disks

 - Low-Level Disk Management

 - Registry Key Monitoring

 - Windows Installation Identification

 - Unique Computer Identification

 - Reads Internet Settings

 - Attempting Multiple Internet Connections

 - Low-Level Disk Write

 - Deleting Another Executable File

 - Deleting Multiple Executable Files (Mass Deletion)

 - Opening an Important File

 - Opening Multiple Important Files

 - Modifying an Important File

 - Modifying Multiple Important Files

 - Deleting an Important File

 - Deleting Multiple Important Files