

# 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](#).

Concise report

Detailed report

Event chain

Dropped files

Screenshots

Performance logs

RESET FILTERS

ALARM TYPES FILTER

INDICATOR	PARAMETER	HASH SHA256	TIME
> New process			2002:19
> Machine fingerprint query	1		2002:19
> New process			2002:20
> Machine fingerprint query	1		2002:20
> Internet settings query	1		2002:27
> Low-level disk access			2002:27
> Machine fingerprint query			2002:29
> File drop			2002:34
> Machine fingerprint query	1		2002:38
> New process			2002:50
> Low-level disk access			2002:53
Executable was set for self-execution (via task scheduler)			2002:57
Time and date of object execution	21:06:55 25-03-2025 (in 4 minutes)) and repeats every 4 minutes		2002:57
Image set for autorun	C:\Windows\System32\mshta.exe C:\Users\Администратор\AppData\Local\Settings\locale		2002:57
Task user name	USER-PC\Администратор		2002:57
Task name	ServiceDispatch		2002:57
Initiator process	C:\Windows\System32\svchost.exe	39f80b...7bf0	2002:57
> Code injection			2003:38

Items per page: 1001 – 13 of 13

Fig. 16 – List of Recorded Activities

RESET FILTERS

ALARM TYPES FILTER

Select all

Select none

New process

Internet settings query

File drop

Code Injection

Machine fingerprint query

Low-level disk access

Executable was set for self-execution (via task scheduler)

Apply

Fig. 17 – Filters for the List of Recorded Activities

Executable was set for self-execution (via task scheduler)

Time and date of object execution	21:06:55 25-03-2025 (in 4 minutes)) and repeats every 4 minutes
Image set for autorun	C:\Windows\System32\mshta.exe C:\Users\Администратор\AppData\Local\Settings\locale
Task user name	USER-PC\Администратор
Task name	ServiceDispatch
Initiator process	C:\Windows\System32\svchost.exe

All actions by process

All actions on process

All actions by process with this name

All actions on process with this name

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.

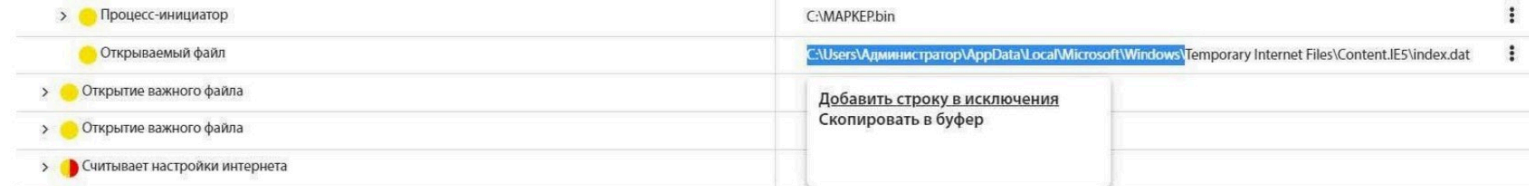


Fig. 18.1 – Defining the File/Directory Exclusion Path

### Add exclusion

Event:	Executable was set for self-execution (via task scheduler)
Parent:	C:\Windows\System32\svchost.exe
Initiator process	C:\Windows\System32\svchost.exe
Exclude path:	<input type="text" value="C:\Windows\System32\svchost.exe"/>
Operating system:	<div>Any</div>
User semantics	<div></div>
<div>SUBMIT</div>	

Fig. 18.2 – Exclusion Addition Window

 [Edit this page](#)