



# Отчеты

Таблица с готовыми отчетами можно отображается при нажатии на кнопку **Отчеты** в верхнем навигационном меню. Число справа на кнопке **Отчеты** информирует о количестве непрочитанных отчетов.

ФИЛЬР ПО ЗАКЛЮЧЕНИЮ		ФИЛЬР ПО ТИПУ ФАИЛОВ		ПРИМЕНИТЬ ФИЛЬРЫ		СБРОСИТЬ ФИЛЬРЫ						СПИСОК ОТЧЕТОВ: 165587		
<input type="checkbox"/>	№ ОТЧЕТА	УРОВЕНЬ УГРОЗЫ	ИМЯ ФАЙЛА	ДАТА И ВРЕМЯ	ХЭШ SHA256	ТИП АНАЛИЗА	ИНДИКАТОРЫ	КОНФИГУРАЦИЯ	ИСТОЧНИК ФАЙЛА	ТЕГИ/ВЕРДИКТ				
<input type="checkbox"/>	389549	<span>0</span>	✓ 1465.pdf	14/04/25 14:23:08	ac84d6			Windows 10 x64 dev	Direct upload					
<input type="checkbox"/>	389280	<span>0</span>	✓ v1800017234.....kaz.pdf	12/04/25 11:35:51	b1d4f0					Browser extension				
<input type="checkbox"/>	386448	<span>0</span>	✓ eb41b8bc1a2d.....0eb0.pdf	12/04/25 11:25:40	eb41b8			Windows 10 x64 o11	Direct upload					
<input type="checkbox"/>	386447	<span>0</span>	✓ eb4083aec53c.....bd7.docx	12/04/25 11:24:40	eb4083			Windows 10 x64 o11	Direct upload					
<input type="checkbox"/>	386446	<span>0</span>	✓ eb39e2e37db9.....28da.pdf	12/04/25 11:23:39	eb39e2			Windows 10 x64 o11	Direct upload					
<input type="checkbox"/>	386445	<span>0</span>	✓ eb3911b9bb46.....135.docx	12/04/25 11:22:39	eb3911			Windows 10 x64 o11	Direct upload					
<input type="checkbox"/>	386444	<span>0</span>	✓ eb36352e7f18.....4924.pdf	12/04/25 11:21:39	eb3635			Windows 10 x64 o11	Direct upload					
<input type="checkbox"/>	386443	<span>0</span>	✓ eb3406bd7dd2.....9a9c.pdf	12/04/25 11:20:38	eb3406			Windows 10 x64 o11	Direct upload					
<input type="checkbox"/>	386442	<span>0</span>	✓ eb3028bcd07f.....00c8.pdf	12/04/25 11:19:38	eb3028			Windows 10 x64 o11	Direct upload					
<input type="checkbox"/>	386441	<span>0</span>	✓ e88bcd186c8.....fc19.pdf	12/04/25 11:18:38	e88bcd			Windows 10 x64 o10	Direct upload					
<input type="checkbox"/>	386440	<span>0</span>	✓ eb1f8e43120e.....f9f.xlsx	12/04/25 11:17:38	eb1f8e			Windows 10 x64 o11	Direct upload					
<input type="checkbox"/>	386439	<span>0</span>	✓ e88a41ea137d.....d96.docx	12/04/25 11:16:37	e88a41			Windows 10 x64 o10	Direct upload					
<input type="checkbox"/>	386438	<span>0</span>	✓ eb12af988421.....e92.docx	12/04/25 11:15:37	eb12af			Windows 10 x64 o11	Direct upload					

Рис. 9 – Список сформированных отчетов

Таблица содержит следующие столбцы:

- Флажок для выделения нескольких отчетов для проведения операции над группой объектов;
- Статус о прочтении отчета;
- Тип анализа (ряд иконок) – динамический, статический;
- Динамический анализ выполняется
- Динамический анализ готов
- Статический анализ готов
- Дата и время генерации отчета;
- Имя файла – ссылка на сам отчет и имя, под которым был загружен файл;
- Значение хэш-функции SHA256 для файла, который можно использовать для быстрого поиска идентичных файлов;
- Индикаторы активности файла (ряд иконок), такие как интернет активность, внедрение в процессы, создание сервисов, запуск на автозагрузку (Список возможных индикаторов приведен

## в Приложении 1.);

- Количество снимков экрана, снятых при динамическом анализе;
- Уровень угрозы, подсчитанный системой tLab в зависимости от объема и вредоносности активностей найденных при динамической анализе. Чем выше значение, тем опаснее файл;
- Индикатор опасности указывает опасность файла на цветовой шкале: зеленый – безопасный, оранжевый – требует внимания, красный – высокая вероятность вредоносности;
- Заключение эксперта или администратора. Заключение выставляется внутри отчета.

При нажатии на кнопку Фильтры отображается дополнительное меню, в котором можно отсортировать список отчетов по различным свойствам или выбрать количество результатов размещаемых на одной странице. Кнопка Выделить все выделяет все отчеты на странице, над которыми затем можно произвести действия: Пометить как прочитанные/непрочитанные или Удалить. Удаленные файлы перемещаются в корзину, доступ к которой имеет только администратор. Случайно удаленные файлы можно восстановить из корзины.

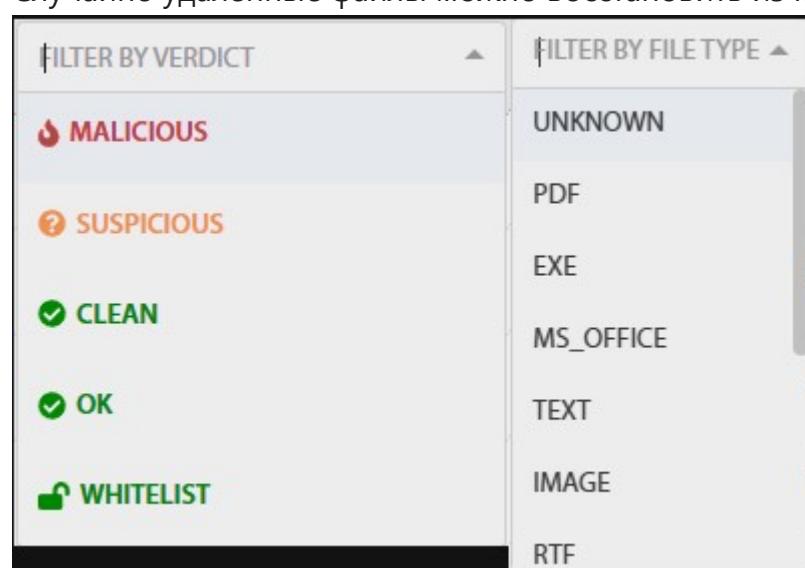


Рис. 10 – Меню фильтров

С ОПРАВИТЬ ФАЙЛ ЗАНОВО СОХРАНИТЬ PDF KILL CHAIN ВСЕ ОТЧЕТЫ ФАЙЛА ЗАКЛЮЧЕНИЕ УДАЛИТЬ СКАЧАТЬ АНАЛИТИКА ОТЧЕТА ОТ GPT ОТЧЕТ #79025

file.exe

Общие сведения

146	Оценка угрозы
Заключение:	UNKNOWN
Оценка угрозы:	146 (potentially 146)
Имя файла:	file.exe
Тип файла:	EXE
Размер файла:	1.03 MB
Загрузил:	script
Время отчета:	10/01/22 12:33:24
Хэш SHA-256:	673b26afda37cf220e9e1fbcbef971be8d630e70f23b066a7a12a254892d2dd
Хэш SHA-1:	06002c90bbabfb4fb7a4e4309f37e918742590e3
Хэш MD5:	40d6e7c951adf91a17bc2bcff2fd55dc
Известное легитимное ПО:	Нет

Индикаторы угрозы

- Массовая активность
- Обнаружение антивирусом

Параметры исполнения

Длительность анализа:	96 сек.
Доступ к интернету:	Нет
Сохранить дамп памяти:	Нет
Версия детектора:	218
Операционная система:	Windows 7 x64 6.1

Рис. 11 – Общий отчет

Страница отчета состоит из трех вертикальных вкладок. Вкладка Общий отчет содержит общую информацию о файле, заключение эксперта и параметры анализа. Вкладка Статический отчет содержит данные собранные статическим анализатором. Вкладка Динамический отчет содержит результаты динамического анализа. При нажатии на кнопку Операции с файлом отображается соответствующее меню, которое содержит следующие пункты:

- Отправить заново (открывает форму повторной отправки файла на анализ);
- История (список всех отчетов с этим файлом, даты-ссылки на отчеты);

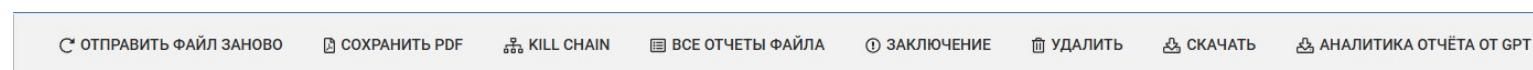


Рис. 12 – Меню операций с файлом

При нажатии на кнопку **Поиск** в навигационном меню открывается страница поиска отчетов в системе. Поиск ведется по многочисленным полям, которые можно увидеть в общем отчете и начало которого показано в соответствующих колонках списков отчетов и очереди. При вводе 4-6 символов в поле поиска SHA256 в поле ввода отображается всплывающий список с присутствующими отчетами, в которых совпадают введенные символы. Для перехода к найденному отчету необходимо ввести полное значение хэшфункции (или выбрать в списке) и нажать кнопку **Поиск**.

Hash SHA-256:	Hash SHA-256	
Hash SHA-1:	Hash SHA-1	
Хэш MD5	Hash MD5	
Имя файла	Filter by file name	
Вердикты	ФИЛЬР ПО ЗАКЛЮЧЕНИЮ	
Статические индикаторы	Фильтр по статическим индикаторам	Все <input type="checkbox"/>
Динамические индикаторы	Фильтр по динамическим индикаторам	Все <input type="checkbox"/>
Тип файла	ФИЛЬР ПО ТИПУ ФАИЛОВ	
Источник файла	Фильтр по источникам файлов	
Тэги:	Фильтр по тегам	
С даты	Выберите дату	
По дату	Выберите дату	

**СБРОСИТЬ** **ПОИСК**

Рис. 13 – Страница поиска отчетов

 [Отредактировать эту страницу](#)