



Загрузка файлов

Загрузка файлов на проверку осуществляется на вкладке Загрузка файлов страницы Загрузка, которая доступна через верхнее навигационное меню. При нажатии на кнопку Выбрать файлы для проверки появится диалоговое окно для выбора файлов любого типа. В диалоговом окне возможен выбор группы файлов через выделение мышью или с помощью комбинации *Ctrl + Левая кнопка мыши*. В данной версии tLab не поддерживается загрузка папок, только индивидуальных файлов.

Выберите файлы для анализа

Дополнительные свойства анализа



Настройки среды

Загрузить предустановку

Выберите предустановку



Сбросить предустановку

Сохранить предустановку

Удалить предустановку

Тип приложения	Операционная система	Версия приложения	Доступные ВМ
НЕ ОПРЕДЕЛЕНО	Windows 10 x64 dev	Any	1
PDF	Windows 10 x64 dev	Any	1
RTF	Windows 10 x64 dev	Any	1
MS_OFFICE	Windows 10 x64 dev	Any	1

ОТПРАВИТЬ

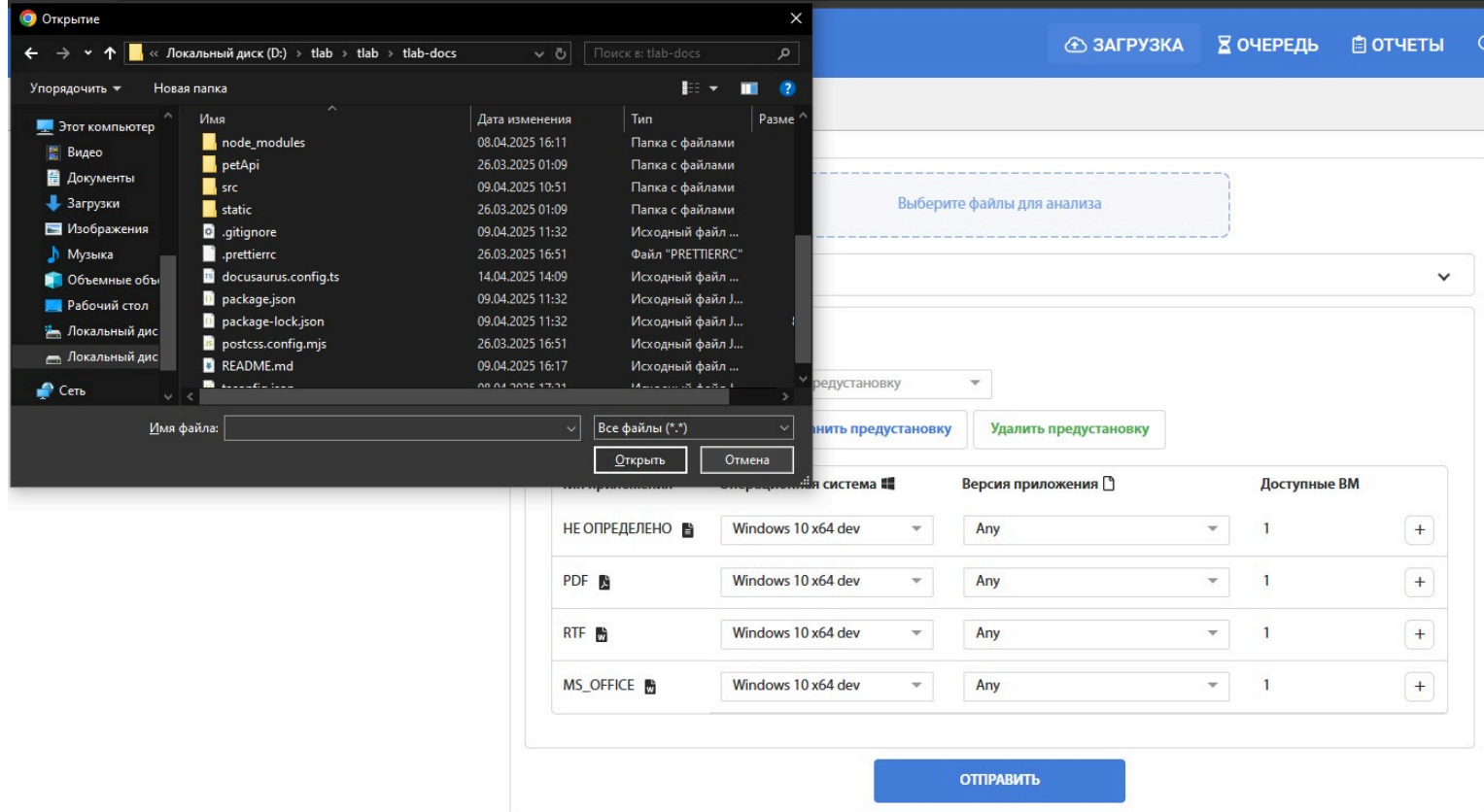


Рис. 2 — Диалог выбора файлов для загрузки

После выбора файлов кнопка Открыть закроет диалоговое окно выбора файлов. При повторных нажатиях Выбрать файлы для проверки можно выбрать файлы находящиеся в разных директориях. Общее количество и общий размер файлов по умолчанию составляют 10 файлов и 100 Мегабайт.

Выберите файлы для анализа

Выберите главный файл

- ☒ Загрузить все файлы отдельно
- ☐ 1465.pdf ✗
- ☐ 10.1007@978-981-13-9155-25.pdf ✗
- ☐ moradpoor2017.pdf ✗

Рис. 3 – Форма загрузки после выбора группы файлов

Отменить выбор файлов (или группы файлов) можно через нажатие красного X рядом с файлом (группой).

При загрузке группы файлов возможно проведение динамического анализа всей группы. Данное свойство необходимо для проверки файлов с зависимостями. Для этого необходимо выбрать главный файл, который будет запущен во время анализа. Тогда остальные файлы будут использоваться в качестве зависимостей и располагаться в одной директории.

Дополнительные свойства анализа

ОБЩИЕ

Общий доступ

OFFON

Приоритет анализа

Low

Поведенческий анализ

OFFON

Игнорировать белый список

OFFON

Распаковка архивов

OFFON

Пароль архива

Password

ДИНАМИЧЕСКИЕ

Длительность анализа

120sec.

Доступ к интернету

OFFON

Переименование файла

OFFON

Ускорение

OFFON

Режим скрытности

OFFON

Командная строка

max 220 char.

ИСПОЛНЕНИЕ

Включить все

Выключить все

rtf dde clicker

Shredder Algo 1

Shredder Algo 1

Shredder GOST Algo

Shredder Test

Shredder_Click_FILE

Pafish23

SharePoint

Добавить скрипт

Рис. 4 – Форма загрузки файлов с дополнительными настройками

Дополнительные свойства анализа позволяет изменить дополнительные настройки анализа. Список возможных свойств:

Доступ – При включении данной опции отчеты выбранных файлов станут доступными для просмотра всем пользователям системы. В ином случае доступ к сформированным отчетам имеет пользователь, загружающий объекты, и администратор.

Приоритет анализа – Позволяет провести более срочные анализы вне очереди.

Тип анализа – Включает или отключает проведение статического и динамического анализов. По умолчанию производятся все виды анализа.

Игнорировать белый список – По умолчанию доверенные файлы не анализируются и появляется сообщение об их доверенном статусе. При включении данной опции производится анализ всех файлов, даже находящихся в белом списке доверенных.

Распаковка архивов – При активации данной опции производится распаковка загружаемых архивов и производится отдельный анализ для каждого объекта, находящегося в архиве. Активации данной

опции никак не влияет на обработку других типов файлов при загрузке.

Пароль архива – Данное поле используется для ввода пароля от архива, в случае его наличия

Длительность анализа – Используется для установки длительности динамического анализа. 2 минуты по умолчанию, максимум 60 минут.

Доступ к интернету – Открывает доступ в сеть интернет из контейнера при динамическом анализе. Требуется осторожность при загрузке вирусов распространяющихся через сеть, таких как WannaCry и Petya. По умолчанию доступ к сети отключен.

Переименование файла – При активации данной опции оригинальное имя загружаемого объекта будет изменено во время динамического анализа. Это имя затем используется в цепочке событий.

Ускорение – При включении данной опции производится нивелирование основных видов задержек, включая трудноустраняемые циклы микрозадержек.

Командная строка – Позволяет указать параметры командной строки для запуска анализируемого файла при динамическом анализе.

Версии – Данная опция дает возможность выбора окружения для динамического анализа для документов Microsoft Office и Adobe Reader. При выборе более одной версии будет создано несколько анализов и формируется несколько отчетов. Для одного анализа следует выбирать окружение из одной группы (например, только из группы Microsoft Office или Adobe Reader).

Сценарии симуляции пользовательской активности – На данной панели происходит выбор сценариев, используемых при динамическом анализе объекта с графическим интерфейсом. У каждого сценария есть имя, условия активации (совпадение по названию окна и/или имени процесса), выполняемые команды, минимальное и максимальное количество повторов команды, задержка перед выполнением действий и задержка между действиями. Сценарии выполняются в порядке сверху вниз, таким образом можно создать и выполнить несколько сценариев по порядку для определенных программ, например, сценарий №1 нажимает кнопку TAB 3 раза, а сценарий №2 нажимает кнопку ENTER

ИСПОЛНЕНИЕ

[Включить все](#)
[Выключить все](#)

☐ rtf dde clicker

☐ Shredder Algo 1

☐ Shredder Algo 1

☐ Shredder GOST Algo

☐ Shredder Test

☐ Shredder_Click_FILE

☐ Pafish23

☐ SharePoint

[Добавить скрипт](#)

Создать новый сценарий

Имя сценария

Названия окна

Если окно

содержит

Названия окна

Если процесс

содержит

Название процесса

Если класс

содержит

Класс окна

Не учитывать регистр

Делать снимок

Choose end actions preset

Действие

Значение

Названия окна

Нажатие ENTER

Значение

Названия окна

Только назначенные действия

Сделать действие как минимум

2

раз(а)

Сделать действие не более

10

раз(а)

Интервал между действиями

500

мс

Задержка перед действиями

3

сек.

ОТПРАВИТЬ

Рис. 5 – Сценарии симуляции пользовательской активности

Внимание!

Файл с названием 1465.pdf был уже проанализирован 26/03/25 18:53:04

[Просмотр ранее загруженного отчета](#)

ОТПРАВИТЬ ЕЩЕ РАЗ

Рис. 6 – Сообщение о повторной загрузке

При повторной загрузке существующего в системе tLab файла появится сообщение с административным заключением, ссылкой-датой на последний отчет и кнопкой Отправить заново, для повторного анализа файла

File 1465.pdf was accepted for analyzing

Заккрыть

Рис. 7 — Сообщение об успешной загрузке файла

Отредактировать эту страницу