



# Kaspersky Research Sandbox

## Песочница

Kaspersky Research Sandbox – это мощный инструмент, который позволяет изучать природу образцов ПО, находить индикаторы компрометации на основе поведенческого анализа и обнаруживать вредоносные объекты, которые не встречались раньше.

# Kaspersky Research Sandbox

Современные целевые атаки все чаще нацелены на определенные компании. Для подготовки атак злоумышленники тщательно изучают свою жертву. Чтобы выявлять такие угрозы и бороться с ними, необходимо анализировать поведение файлов, память процессов, сетевую активность и многое другое.

Современные вредоносные программы всеми силами стараются остаться незамеченными. Их код не будет выполнен, если есть хоть малейшая вероятность обнаружения. Так, если система жертвы не соответствует определенным критериям, вредоносная программа практически наверняка самоуничтожится, не оставив следов. Чтобы вредоносный код показал себя, песочница должна уметь точно имитировать поведение обычного пользователя.

Песочница «Лаборатории Касперского» Kaspersky Research Sandbox создана на основе нашего внутреннего комплекса технологий, над которым мы работаем уже более 10 лет. Этот продукт объединил все знания о поведении вредоносного ПО, накопленные «Лабораторией Касперского» в ходе непрерывных исследований угроз. В том числе с его помощью мы каждый день обнаруживаем более 380 000 новых вредоносных объектов. Локальное развертывание, благодаря которому данные не покидают среду организации.

Kaspersky Research Sandbox предлагает гибридный подход, сочетающий в себе поведенческий анализ, надежные техники предотвращения уклона от анализа и технологии моделирования поведения человека. Кроме того, песочница «Лаборатории Касперского» позволяет настраивать образы систем для анализа так, чтобы они соответствовали реальной инфраструктуре, что повышает точность обнаружения угроз и скорость расследования.

## Преимущества продукта

Автоматизированный анализ объектов в средах Windows, Linux и Android

Возможность кастомизировать образы ОС, позволяющая анализировать реальные угрозы для разных ОС и приложений

Определение рейтинга угроз и уровня опасности анализируемого объекта по метрикам и данным, полученным в результате исполнения файла

Локальное развертывание, благодаря которому данные не покидают среду организации

Предотвращение уклонения от анализа и эмуляция активности пользователей

Отправка файлов вручную и API на основе REST

Поддержка анализа более сотни типов файлов

Пользовательские правила Suricata для проверки сетевого трафика, которые можно применять наряду с правилами Suricata, настроенными поставщиком

Возможность развертывания на «пустых» машинах без ОС и простое масштабирование с учетом требований к производительности

## Высокоуровневая архитектура Kaspersky Research Sandbox



Продукт поддерживает развертывание на «пустых» машинах без ПО. Аппаратная конфигурация зависит от требований к производительности. При этом ее можно масштабировать. Необходима скорость подключения 100 Мбит/с для каждого канала и хотя бы одно подключение через независимого интернет-провайдера (а лучше два или более в целях отказоустойчивости). Интернет-провайдер должен быть готов к вредоносному трафику.

Продукт Kaspersky Research Sandbox основан на патентованной технологии «Лаборатории Касперского» (№ патента US10339301). Песочница воссоздает условия для запуска вредоносного кода, чтобы исследователи могли с первой попытки проанализировать подозрительный файл или URL-адрес.

Чтобы остаться незамеченным, вредоносный файл сначала старается выяснить, находится ли он в виртуальной машине, либо бездействует, пока не перестанет работать песочница. В таких случаях наша запатентованная технология ускоряет течение времени в виртуальной машине, чтобы вредоносный код был выполнен раньше.

Если целью является приложение, которого нет в песочнице, программа не запустит свой код. Чтобы решить эту проблему, исследователям нужно изучить журналы, понять, чего не хватает, добавить это в виртуальную машину и повторить процесс. Вот как это происходит: вредоносное ПО попытается получить доступ к приложению, а система перехватывает эту попытку. Она не дожидается окончания выполнения файла, а приостанавливает процесс, чтобы создать нужное приложение и ресурсы.

---

# Подробные аналитические отчеты

После завершения анализа песочница создает подробный отчет о поведении и функциях образца, чтобы вы могли реализовать подходящие ответные меры. Отчет содержит следующие сведения:

## Заключение

Общая информация о результатах выполнения файла или проверки URL-адреса.

## Карта выполнения

Графически представленные действия объекта и взаимосвязи между ними.

## Загруженные PE-образы

Список загруженных PE-образов, обнаруженных во время выполнения файла или проверки URL-адреса.

## Операции с процессами

Список взаимодействий с процессами, зарегистрированных во время выполнения файла.

## Внедренные файлы

Список файлов, которые были сохранены (созданы или изменены) выполняемым файлом.

## Матрица MITRE ATT&CK

Вся активность процессов, зарегистрированная во время эмуляции, представленная в форме матрицы MITRE ATT&CK.

## Обнаружения

Список обнаружений (поведенческих и касающихся противодействия вредоносному ПО), зарегистрированных при выполнении файла.

## Подозрительная активность

Список зарегистрированных подозрительных действий.

## Файловые операции

Список файловых операций, зарегистрированных во время выполнения файла, проверки URL-адреса.

## Операции синхронизации

Список операций создаваемых объектов синхронизации (мьютекс, событие, семафор), зарегистрированных во время выполнения файла или проверки URL-адреса.

## HTTPS/HTTP/DNS/IP/TCP/UDP и др.

Сведения о сетевых сеансах / запросах, зарегистрированных во время выполнения файла или проверки URL-адреса.

## Сработавшие сетевые правила

Список сетевых правил Suricata, которые сработали во время анализа трафика от запущенного объекта.

## Создание снимков экрана

Набор снимков экрана, сделанных во время выполнения файла или проверки URL-адреса.

## Операции с реестром

Список операций с реестром ОС, обнаруженных во время выполнения файла или проверки URL-адреса.

## Загруженные файлы

Список файлов, извлеченных из сетевого трафика во время выполнения файла или проверки URL-адреса.

## Дамп сетевого трафика (PCAP)

Сетевая активность, которую можно экспортировать в формате PCAP.

**Kaspersky Research Sandbox – это оптимальный инструмент для обнаружения неизвестных угроз. У этого продукта есть все необходимое для противодействия продвинутым угрозам.**



## Kaspersky Research Sandbox

[Подробнее](#)

[www.kaspersky.ru](http://www.kaspersky.ru)

© 2022 АО «Лаборатория Касперского».  
Зарегистрированные товарные знаки и знаки обслуживания  
являются собственностью их правообладателей.