kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Research Sandbox

Современные комплексные угрозы 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. 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.

Преимущества продукта

- Локальное развертывание, благодаря которому данные не покидают среду организации
- Поддержка анализа более сотни типов файлов
- Предотвращение уклонения от анализа
- Эмуляция активности пользователей
- Поддержка ОС Windows и Android
- Возможность кастомизировать образы ОС, позволяющая анализировать реальные угрозы для разных ОС и приложений
- Подробные аналитические отчеты, включающие все системные процессы, извлеченные файлы, сетевую активность (PCAP) и наглядные графики
- Интеграция с Kaspersky Private Security Network
- Отправка файлов вручную и API на основе REST для безупречной интеграции и автоматизации мер безопасности

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

Песочница 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. С его помощью мы каждый день обнаруживаем более 350 000 новых вредоносных объектов.

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 исследования. При локальном развертывании песочницы важные данные не покидают среды организации.

На диаграмме ниже показана высокоуровневая архитектура Kaspersky Research Sandbox.

Высокоуровневая архитектура Kaspersky Research Sandbox

Чтобы остаться незамеченным, вредоносный файл сначала старается выяснить, находится ли он в виртуальной машине, или 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, вредоносная 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. Если вредоносное ПО попытается получить доступ к приложению, запатентованная система перехватит эту попытку. Система не дожидается окончания выполнения файла, а приостанавливает процесс, чтобы создать нужное приложение и ресурсы.

Правила обнаружения, которые предписывают, как реагировать на определенное событие, не предустановлены и не реализованы внутри модуля, но их можно добавлять и обновлять.

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

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.

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

- **Сводка** – общая информация о результатах выполнения файла.
- **Список детектов** – список антивирусных и поведенческих детектов, зарегистрированных песочницей при выполнении файла.
- **Срабатывания сетевых правил** – список сетевых правил SNORT, которые сработали во время анализа трафика от запущенного объекта.
- **Дерево выполнения** – графически представленная последовательность действий объекта (действия, выполненные с файлами, процессами и реестром, а также сетевая активность) и взаимосвязи между ними. Корневой узел дерева представляет выполненный объект.
- **Подозрительные действия** – список зарегистрированных подозрительных действий.
- **Снимки экрана** – набор снимков экрана, сделанных во время выполнения файла.
- **Загруженные образы PE** – список загруженных образов PE, обнаруженных во время выполнения файла.
- **Файловые операции** – список файловых операций, зарегистрированных во время выполнения файла.
- **Операции с реестром** – список операций с реестром ОС, обнаруженных во время выполнения файла.
- **Операции с процессами** – список взаимодействий файла с различными процессами, зарегистрированных во время выполнения файла.
- **Операции синхронизации** – список операций создаваемых объектов синхронизации (мьютекс, событие, семафор), зарегистрированных во время выполнения файла.
- **Загруженные файлы** – список файлов, извлеченных из сетевого трафика во время выполнения файла.
- **Созданные файлы** – список файлов, которые были сохранены (созданы или изменены) выполняемым файлом.
- **Запросы HTTPS/HTTP/DNS** – списки запросов HTTPS/HTTP/DNS, зарегистрированных во время выполнения файла.
- **Дамп сетевого трафика (PCAP)** – сетевая активность, которая может быть экспортирована в формате PCAP.

Kaspersky Research Sandbox – это оптимальный инструмент для обнаружения неизвестных и сложных угроз.

www.kaspersky.ru