kaspersky BRING ON THE FUTURE

Kaspersky Research Sandbox

Принятие интеллектуального решения на основе поведения файла с одновременным анализом памяти процесса, сетевой активности и т. д., является оптимальным подходом к пониманию современных сложных целенаправленных угроз. Технологии исследовательской песочницы - это мощные инструменты, позволяющие исследовать происхождение образцов файлов, собирать IOC на основе поведенческого анализа и обнаруживать ранее невиданные вредоносные объекты.

Основные характеристики продукта:

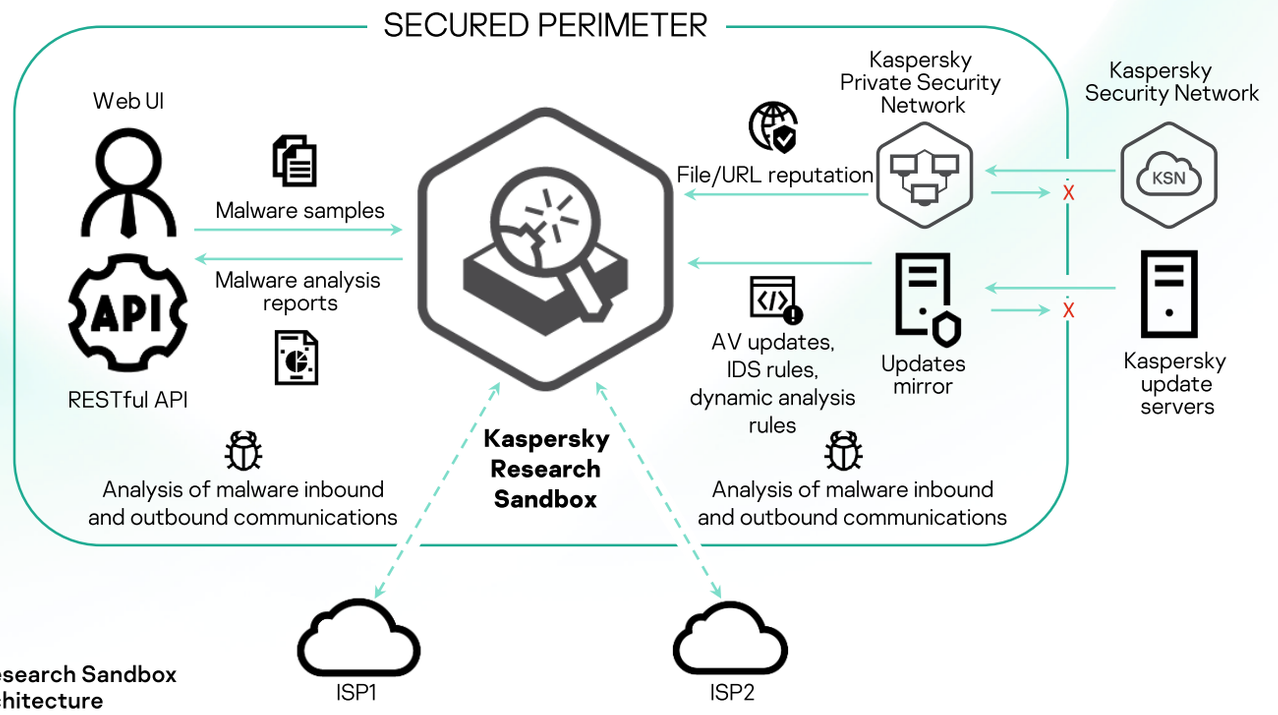
- Локальное развертывание гарантирует, что никакие данные не будут доступны за пределами организации.
- Поддерживает анализ более чем ста типов файлов.
- Передовые методы борьбы с уклонением от обнаружения
- Эмуляция активности пользователей.
- Пользовательские изображения, позволяющие анализировать угрозы в различных операционных системах.
- Отдельный анализ каждого процесса для выявления подозрительных действий с помощьюсоответствующих сетевых подключений
- Детальный анализ отчетов, включая все системные действия, извлеченные файлы, сеть деятельность (PCAP) и визуальные графики.
- Экспорт данных в формате STIX, JSON и CSV.
- Поддержкаинтеграциис Kaspersky Private Security Network.
- Ручная подача файлов и RESTful API для бесшовной интеграции и автоматизации ваших операций по обеспечению безопасности.
- Расширенные журналы песочницы и дампы (для продвинутых пользователей)

Сегодняшнее вредоносное ПО использует целый ряд методов, чтобы избежать выполнения своего кода, если это может привести к раскрытию его вредоносной активности. Если система не соответствует требуемым параметрам, то вредоносная программа почти наверняка уничтожит себя, не оставив никаких следов. Поэтому для выполнения вредоносного кода среда песочницы должна быть способна точно имитировать нормальное поведение конечного пользователя.

Песочница Kaspersky Research Sandboxразработана непосредственно из нашего лабораторного комплекса для песочницы как технологии, которая развивается уже более десяти лет. Она включает в себя все знания о поведении вредоносных программ, полученные Лабораторией Касперского в ходе наших непрерывных исследований угроз, что позволяет нам обнаруживать более 350 000 новых вредоносных объектов каждый день. Развернутая локально, эта мощная технология также предотвращает раскрытие данных за пределами организации.

Kaspersky Research Sandbox предлагает гибридный подход, сочетающий поведенческий анализ и твердую защиту от уклонения с технологиями моделирования человеческого поведения. Она также позволяет настраивать образы систем для анализа, адаптируя их к вашим реальным условиям, что повышает точность обнаружения целевых угроз и скорость расследования.

Приведенная ниже схема описывает высокоуровневую архитектуру песочницы Kaspersky Research Sandbox.



Kaspersky Research Sandbox high-level architecture

Чтобы избежать разоблачения, вредоносный файл может сначала проверить, находится ли он в виртуальной машине или остается неактивным в течение определенного периода времени, пока песочница не перестанет работать. В таких случаях запатентованная технология ускоряет течение времени внутри виртуальной машины, поэтому вредоносный код вынужден выполняться раньше.

Вредоносное ПО может не показывать свое вредоносное поведение, если оно нацелено на конкретное приложение, которое отсутствует в песочнице. Чтобы решить эту проблему, исследователи должны просмотреть журналы, понять, что отсутствует, добавить его в виртуальную машину и запустить этот процесс снова. При этом, когда вредоносное ПО пытается получить доступ к приложению, запатентованная система перехватывает эту попытку. Он не дожидается завершения выполнения файла, а приостанавливает процесс создания необходимого приложения, а также содержимого.

Правила обнаружения, описывающие, как реагировать на определенное событие, не устанавливаются заранее и не реализуются внутри движка, но могут быть легко обновлены и добавлены.

- осуществление проверки файлов в Windows XP, Windows 7, Windows 8.1, Windows 10;
- осуществление проверки файлов следующих форматов: .exe, . dll, .bat, .pdf, .doc, .docx, .docm, .dotm, .rtf, .zip, .7z, .rar, .vbs, .xls, .xlsx, .xlsm, .ppt, .pptx, .pptm, .pps, .ppsx, .ppsm, .js, .html, .jar, .java, .msi, .bzip2, .gzip, .arj, .iso, .cab, .msg, .eml, .psl, .sh;
- возможность проведения эвристического анализа исполняемых скриптов, а также файлов документов в следующих форматах: .doc, .docx, .xls, .xlsx, .ppt, .pptx, .pdf.

Песочница Kaspersky Research основана на запатентованной фирменной технологии (патент US10339301). Создавая точные условия, которые запускают вредоносное ПО, она позволяет исследователям проанализировать подозрительный файл за одну попытку.

Конфигурация оборудования зависит от требуемой производительности и может быть масштабирована. Для этого требуется сетевое соединение 100 Мбит / С для каждого канала и по крайней мере одно независимое подключение (два или более рекомендуется для обеспечения отказоустойчивости). Провайдердолженбытьосведомлениготовквредоносномутрафику. Конфигурация оборудования зависит от требуемой производительности и может быть масштабирована. Для этого требуется сетевое соединение 100 Мбит / С для каждого канала и по крайней мере одно независимое подключение (два или более рекомендуется для обеспечения отказоустойчивости). Провайдер должен быть осведомлен и готов к вредоносному трафику.

После завершения анализа Research Sandbox предоставляет подробный отчет о поведении и функциональности анализируемого образца, позволяющий определить соответствующие процедуры реагирования:

• **Сводка** - Общая информация о результатах выполнения файла.

• **Названия детектов песочницы** - список детектов (как AV, так и поведенческих), которые былизарегистрированы во время выполнения файла.

• **Триггерные сетевые правила** - список правил SNORT, которые были вызваны при анализе трафика от выполняемого объекта.

• **Карта исполнения** - графически представленная последовательность действий объекта (влияния на файлы, процессы и реестр, а также сетевую активность) и связьмежду ними.

• **Подозрительные действия** - список зарегистрированных подозрительных действий.

• **Скриншоты** - набор скриншотов, которые были сделаны во время выполнения файла.

• **Загрузка среды предустановки** — список загруженных образов среды предустановки, которые были обнаружены в исполняемом файле;

• **Файловые операции** - список файловых операций, которые были зарегистрированы во время исполнения файла.

• **Операции реестра** — список операций, выполненных в реестре операционной системы, которые былиобнаружены во время выполнения файла.

• **Операции процесса** - список взаимодействий файла с различными процессами, которые были зарегистрированы во время выполнения файла.

• **Синхронизация операций** - мсписок операций созданных объектов синхронизации (mutex, event, semaphore, которые были зарегистрированы во время выполнения файла.

• **Загруженные файлы** - список файлов, которые были извлечены из сетевого трафика во времявыполнения файла.

• **Удаленные файлы** - список файлов, которые были сохранены (созданы или изменены) исполняемым файлом.

• **Запросы HTTPS / HTTP / DNS** - списки запросов HTTPS/HTTP / DNS, которые были зарегистрированы во время выполнения файла.

• **Дамп сетевого трафика (PCAP)** - сетевая активность, которая может быть экспортирована в формате PCAP.

Kaspersky Research Sandbox-это инструмент выбора для обнаружения неизвестных угроз. Это.более зрелый и более ориентированный на передовые угрозы подход, чем любое другое решение.

Cyber Threats News: www.securelist.com
IT Security News: business.kaspersky.com
IT Security for SMB: kaspersky.com/business
IT Security for Enterprise: kaspersky.com/enterprise

www.kaspersky.com

2019 AO Kaspersky Lab. All rights reserved.
Registered trademarks and service marks are the property of their respective owners.

We are proven. We are independent. We are transparent. We are committed to building a safer world, where technology improves our lives. Which is why we secure it, so everyone everywhere has the endless opportunities it brings. Bring on cybersecurity for a safer tommorow.

Know more at kaspersky.com/transparency

Proven.
Transparent.
Independent.