Kaspersky Cloud Sandbox

kaspersky АКТИВИРУЙ БУДУЩЕЕ

Kaspersky Cloud Sandbox
Облачная песочница

Принятие аналитического решения на основе поведения файла при одновременном анализе памяти процессов, сетевой активности и прочих показателей – это оптимальный подход к пониманию современных комплексных целевых и APT-угроз.

Запрос пробного доступа к Kaspersky Cloud Sandbox

Подробнее

Современные целевые атаки невозможно предотвратить, используя только традиционные превентивные инструменты. Антивирусный движок способен останавливать только известные угрозы и их разновидности, в то время как создатели вредоносного ПО пускают в ход все средства, чтобы скрыть его от автоматического обнаружения. При этом убытки от киберинцидентов могут составлять десятки миллионов рублей, поэтому важно быстро обнаруживать угрозы и реагировать до нанесения ими серьезного ущерба.

В статистических данных часто не хватает информации о недавно измененных вредоносных программах. В то же время, технологии песочницы – это мощный инструмент, который позволяет исследовать исходные образцы файлов, находить индикаторы компрометации на основании поведенческого анализа и обнаруживать вредоносные объекты, которые не встречались ранее.

Веб-интерфейс

REST API

- Стандартные и расширенные настройки для оптимизации производительности
- Расширенный анализ файлов различных форматов
- Визуализация и интуитивно понятная отчетность
- Блокирование обхода механизмов обнаружения и моделирование активности пользователей

- Расширенное обнаружение APT-, целевых и сложных угроз
- Рабочий процесс, позволяющий проводить действенное и всестороннее расследование инцидентов
- Масштабирование без необходимости покупать дорогостоящие устройства
- Безупречная интеграция и автоматизация процессов безопасности

Проактивное выявление и предотвращение угроз

Комплексная отчетность:

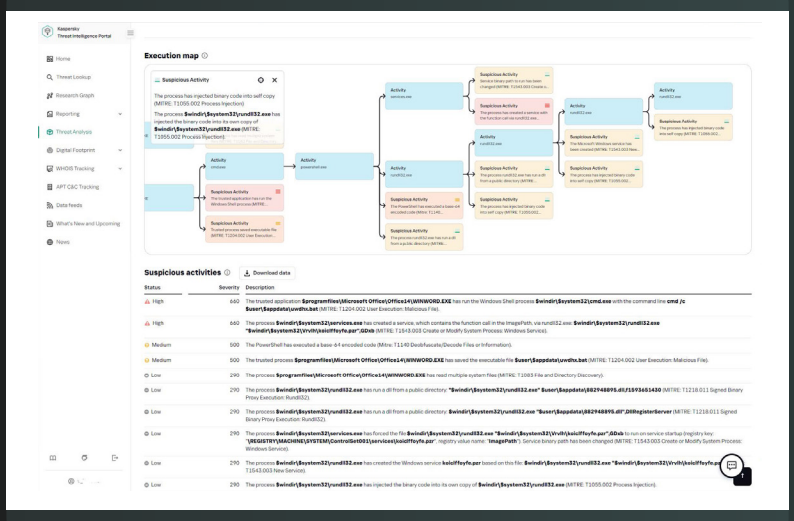
- Загрузка и запуск библиотек DLL
- Внешнее соединение с доменными именами и IP-адресами
- Создание, изменение и удаление файлов
- Подробная информация об угрозах с рекомендациями для каждого выявленного индикатора компрометации
- Дампы памяти процессов и сетевого трафика (PCAP)
- Запросы и ответы HTTP и DNS
- Создание взаимных исключений (мьютексы)
- REST API
- Изменение и создание ключей реестра
- Создание процессов с помощью выполняемого файла
- Снимки экрана
- И многое другое

При выполнении вредоносных программ используются различные методы обхода механизмов обнаружения. Если система жертвы не отвечает определенным критериям, вредоносная программа самоуничтожится, не оставив следов. Для выявления вредоносного кода песочница должна уметь точно имитировать поведение обычного пользователя.

В изолированной среде проводится поведенческий анализ и используются надежные механизмы блокировки таких методов. Также песочница применяет технологии моделирования поведения человека, такие как автокликер, прокрутка документов, и другие действия.

Облачная песочница «Лаборатории Касперского» объединяет все знания о поведении вредоносных программ, полученные за более чем 20 лет непрерывного исследования угроз, что позволяет обнаруживать более 380 000 новых вредоносных объектов каждый день.

Kaspersky Cloud Sandbox является важным компонентом для анализа угроз. В рамках сервиса Kaspersky Threat Lookup собираются подробные актуальные сведения об угрозах: веб-адреса, домены, IP-адреса, хеши файлов, названия угроз, статистические и поведенческие данные, данные WHOIS/DNS и прочие. Облачная песочница позволяет связать эти данные с индикаторами компрометации, сгенерированными анализируемым образцом.



Благодаря Kaspersky Cloud Sandbox можно провести высокоэффективное сложное расследование инцидентов, сразу понять характер угрозы и благодаря интеграции с сервисом Kaspersky Threat Lookup объединить собранные в ходе расследования данные в общую картину, выявляя взаимосвязанные индикаторы угрозы.

Облачная песочница сокращает время реагирования на инциденты и повышает эффективность криминалистического расследования, обеспечивая масштабируемость при автоматической обработке файлов без необходимости и беспокоиться о системных ресурсах.

Kaspersky Threat Intelligence

FORRESTER®

«Лаборатория Касперского» признана лидером по результатам исследования внешних сервисов анализа угроз (Forrester Wave™: External Threat Intelligence Services, Q1 2021)

«Лаборатория Касперского» предлагает сервисы информирования об угрозах, которые открывают доступ к различной информации, полученной нашими аналитиками и исследователями мирового класса. Эти данные помогут любой организации эффективно противостоять современным киберугрозам.

Наша компания обладает глубокими знаниями, богатым опытом исследования киберугроз и уникальными сведениями обо всех аспектах IT-безопасности. Благодаря этому «Лаборатория Касперского» стала доверенным партнером правоохранительных и государственных организаций по всему миру, в том числе Интерпола и различных подразделений CERT. Kaspersky Threat Intelligence предоставляет актуальные технические, тактические, операционные и стратегические данные об угрозах.

Kaspersky Threat Intelligence

Подробнее

www.kaspersky.ru