УДК 004.415.53

VinDoctor – средство изолированного запуска приложений

Винокуров А.А., Доценко Е.В.

Национальный детский технопарк,
г. Минск, Республика Беларусь

Научные руководители: Белоусова Е.С.– кандидат технических наук, доцент кафедры ЗИ;
Мальцев В.Л. – заведующий лаборатории «Информационная безопасность»
Национального детского технопарка

Аннотация. В материалах доклада представлены результаты разработки средства изолированного запуска приложений VinDoctor. На основе изучения общей схемы работы современных SandBox и анализа их достоинств и недостатков был разработан алгоритм работы и пользовательский интерфейс средства изолированного запуска приложений VinDoctor. Тестирование разработанного средства показало, что VinDoctor не оказывает влияния на работу всей

операционной системы в целом по сравнению с существующими аналогами.

Ключевые слова: SandBox, средство изолированного запуска, вредоносные файлы, съемный носитель

Введение. Средство изолированного запуска приложений (Sandbox, песочница) – это выделенная аппаратная или аппаратно-программная среда для исполнения файлов программ. Такая технология применяется, как правило, для эмуляции работы подозрительного программного кода в изолированной среде с целью снижения вероятности нарушения работы продуктивных систем.

Общая схема работы SandBox включает следующие этапы:

1 Начало работы. Запуск, инициализация окружения, проверка доступности системных ресурсов.

2 Изоляция процессов. Создание изолированного контейнера, ограничение доступа к фалойвой системе.

3 Контроль доступа. Определение политик контроля доступа для управления действиями приложения.

4 Мониторинг. Отслеживание активности приложения в реальном времени, регистрация попыток доступа к ресурсам и изменениям в системе.

5 Обнаружение и предотвращение угроз. Реализация механизмов обнаружения вредоносных действий в SandBox.

6 Завершение работы. Остановка и завершение изолированного окружения.

Таким образом, использование средства изолированного запуска приложений позволяет выявить неизвестные типы кибератак на основании поведенческого анализа вредоносного программного обеспечения.

Сегодня на рынке Sandbox производители предлагают несколько видов реализации средств изолированного запуска приложений: решение на базе аппаратной платформы или решение на базе облачного сервиса. Сравнительный анализ современных Sandbox (Comodo Free Antivirus, 360 Total Security) показал, что они являются неэффективными при проверке вредоносных файлов на внешних съемных носителях, содержащих неизвестные сигнатуры и используемые для реализации кибератак типа zero-day. Так, например, Comodo Free Antivirus вообще не определил на съемных носителях вредоносные файлы, а 360 Total Security определяет только сигнатурные вирусы, но при этом пропускает вредоносные файлы, посредством которых нарушитель может получить доступ к операционной систему и управлять ее элементами. Поэтому на основе проведенного анализа существующих SandBox решений было сформулировано предложение разработать новое средство изолированного запуска, в котором не будет всех представленных выше недостатков, которое будет способно выявлять вредоносные файлы разных видов.

Основная часть. Для реализации средства изолированного запуска приложений VinDoctor был разработан алгоритм работы программы (рисунок 1).

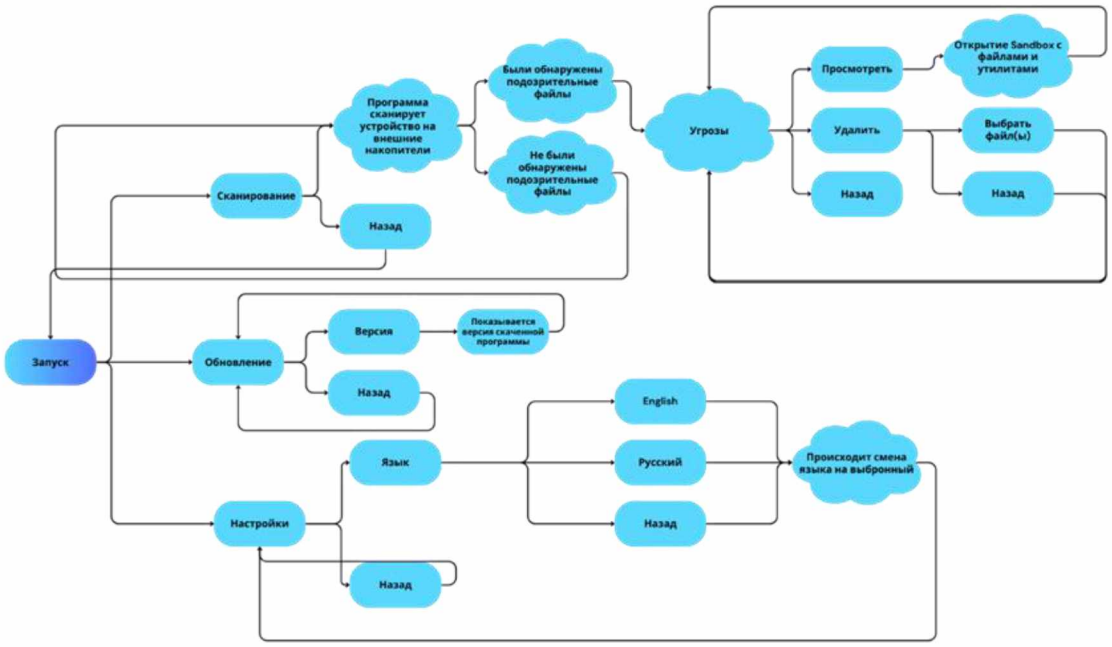

Рисунок 1 – Алгоритм работы средства изолированного запуска приложений VinDoctor

С помощью языка программирования Java (JDK21) был создан эргономичный пользовательский интерфейс средства изолированного запуска приложений VinDoctor, представленный на рисунке 2. Сканер для внешних накопителей был написан на языке программирование Python 3.9.5.

Рисунок 2 – Пользовательский интерфейс средства изолированного запуска приложений VinDoctor

Для проведения тестирования программного решения был разработан код на языке Python 3.9.5. Цель тестирования заключалась в систематическом измерения нагрузки на центральный процессор (ЦП), оперативную память и диск при работе со средством изолированного запуска приложений. При проведении тестирования пользователь активно взаимодействовал с программой VinDoctor, используя все её

возможности, а именно: изменял настройки программы, осуществлял сканирование внешнего носителя с вредоносным файлом и др.

Заключение. В результате тестирования было установлено, что при сканировании внешнего накопителя с вредоносным файлом программой VinDoctor незначительно увеличивается нагрузка на ЦП. Получено, что средняя нагрузка на ЦП составляет 8,27 %, максимальная – 24,9 %, что говорит о том, что разработанное средство изолированного запуска приложений VinDoctor не оказывает влияние на работу всей операционной системы в целом по сравнению с существующими аналогами.

Список литературы

1. Терехов, С.Технология Sandbox как средство обеспечения кибербезопасности электронных государственных услуг / С. Терехов, Д. Шмырев // CONNECT. Мир информационных технологий. – № 9, 2017. – С. 106–109.

2. Антивирусные песочницы [Электронный ресурс]. – Режим доступа : https://habr.com/ru/articles/105581/– Дата доступа : 11.02.2024.

UDC 004.415.53

VINDOCTOR – ISOLATION LAUNCHING APPLICATIONS INSTRUMENT

Vinokurov A.A., Docenko E.V.

National Children's Technopark, Minsk, Republic of Belarus

Belousova E.S. – PhD (Tech.), associate professor at the information security department;
Maltsau V.L. – Head of the information security laboratory at National Children's Technopark'

Annotation. The results of developing for Isolation Launching Applications Instrument VinDoctor was presented in this article. The operating algorithm and user interface for the VinDoctor isolated application launcher were developed based on a studying of the general operating scheme of modern SandBoxes and an analysis of their advantages and disadvantages. Testing of the developed instrument VinDoctor showed that it does not affect the operating system in comparison to analogues.

Keywords: SandBox, Isolation Launching Applications Instrument, malicious files, flash memory card