БАЛТИЙСКИЙ НАУЧНО-ИНЖЕНЕРНЫЙ КОНКУРС 2022
Санкт-Петербург, 21-26 марта 2022 года

Разработка антивирусного ПО против нерешённой уязвимости BAD USB

«Системное программирование и компьютерные технологии»

Батовкин Александр Егорович, Зубов Максим Сергеевич (научный руководитель, учитель информатики), место выполнения работы: В школе и дома

Задачи: Разработать алгоритмы обнаружения и отражения атаки BAD USB; написать программу с применением данных алгоритмов; продемонстрировать эффективность работы написанной программы; распространить ПО, а именно, создать дистрибутивы, подготовить документацию по применению, разместить материалы в публичном доступе. Значимость: На сегодняшний день не существует эффективного метода по борьбе с BAD USB, из-за чего, даже самые популярные антивирусы демонстрируют свою нерезультативность, что доказано экспериментально в работе, а также ведущими экспертами в области информационной безопасности. Как следствие, хакеры пользуются этим и наносят колоссальный ущерб информационной безопасности человечества. Определения и термины: BAD USB – это атака методом злонамеренного использования портов USB в системе путём эмулирования ввода вредоносных команд с недостоверного устройства.

Методы противодействия BAD USB: 1) обнаружение атаки путём анализа поступающей в систему информации, выявление подозрительных паттернов поведения; 2) отражение атаки путём видоизменения вредоносных команд на лету к невыполняемому виду и блокирование ввода в систему на определённое время. Инструменты исследования: программа для эмуляции - VMware Workstation Pro, устройство Raspberry Pi Pico для создания реального прототипа BAD USB.

Были разработаны алгоритм противодействия угрозе BAD USB и антивирусная программа USB Antivirus в трёх распространяемых дистрибутивах: для использования на домашних ПК, в коммерческих и некоммерческих (школы, ВУЗы и т.д.) организациях; также был разработан сайт resoftware.ru, где можно получить информацию об угрозе и программе, а также установить её.

Таким образом, в ходе работы удалось решить одну из самых больших угроз в сфере информационной безопасности. Полученная антивирусная программа определённо может пользоваться спросом, ввиду отсутствия аналогов. В дальнейшем, в поставленные задачи могут войти: добавление в программу различных локализаций для дистрибуции продукта за пределами РФ, создание алгоритма по противодействию аналогичной атаке на устройствах, не использующих клавиатуру.