**Проект "Добрый вирус"**

***Цель проекта:*** научить людей защищаться от вредоносных программ

***Задачи:***

* создать простой вирус, открывающий при запуске устройства веб-страницу о вредоносных программах, защите от их заражения
* создать веб-страницу о вредоносных программах и защите от их заражения

**Заметки**

Написал легкий вирус на C++

Замаскировал полезную нагрузку под популярный Яндекс Браузер, так как в диспетчере задач фоновый процесс называется browser.exe и под него легче замаскировать вредоносное ПО

Не полностью замаскировал вирус, так как проект разрабатывался в целях обучения защиты от вирусов и заменил browser на brovser

Вредоносная программа передается на ПК в виде скрытой папки(good\_folder) и файла sakura.jpg.exe

Содержимое папки good\_folder:

* notification.exe
* brovser.exe
* sakura.jpg

При открытии файла sakura.jpg.exe:

* открывается картинка sakura.jpg
* создается папка Brovser в директории C:\Users\%USERNAME%\AppData\Local
* вредоносные файлы(good\_folder, sakura.jpg.exe) копируются в эту директорию
* в папку автозагрузки копируется файл brovser.exe

Файл brovser.exe (скомпилированный brovser.cpp) открывает файл notification.exe(скомпилированный notification.cpp) каждый час, а также при подключении сьемных носителей копирует вредоносные файлы

**Компиляция**

Файлы .res нужны для добавления иконки приложения

Компилировал проект при помощи G++

**Реакция антивирусов**

* Kaspersky: при копировании файлов в AppData\Local удаляет исполняемый файл sakura.jpg.exe