Создание Винлокера

Введение

В ходе выполнения работы была поставлена учебная задача разработать программу, вредоносного ПО типа «винлокер» (экранный блокировщик). Основная цель заключалась в изучении механизмов блокировки системы и техник социальной инженерии. Для достижения этой цели проект был разделён на несколько взаимосвязанных подзадач:

1. Создать полноэкранное окно, блокирующее доступ к системе;
2. Реализовать механизм автозагрузки программы;
3. Изучить методы маскировки программы под легитимный файл.

Выбор инструментов разработки

Для проведения работы был выбран язык программирования Python 3 с использованием библиотеки Tkinter для создания графического интерфейса. Python был выбран благодаря своей простоте, кроссплатформенности и широким возможностям для системного программирования. В качестве целевой операционной системы рассматривалась Windows 10/11.

Создание полноэкранного окна, блокирующего доступ к системе

Для этой задачи мы использовали библиотеку Tkinter. Она позволила создать окно, которое не отображается на панели задач и не закрывается привычными способами, также оно постоянно находится на переднем плане и загораживает любое приложение, которое пользователь может открыть, например диспетчер задач.

Реализация механизма автозагрузки

Эта подзадача потребовала изучения структуры автозагрузки в Windows. Было установлено, что путь к папке автозагрузки текущего пользователя находится по адресу: %APPDATA%\Microsoft\Windows\Start Menu\Programs\Startup.

Была создана функция add_to_startup_folder(), которая выполняет следующие действия:

1. Определяет путь к исполняемому файлу программы
2. Копирует его в папку автозагрузки
3. Проверяет, не был ли файл уже добавлен ранее

Ключевой особенностью реализации стала проверка if getattr(sys, 'frozen', False), которая корректно работает как при запуске из исходного кода, так и из скомпилированного исполняемого файла.

Маскировка файла

Эта задача стала самой интересной во всей работе. Мы решили, попробовать спрятать наш вирус в картинку, но это оказалось достаточно сложной задачей, тогда на просторах интернета мы нашли информацию про самораспаковывающийся архив. Мы создаём этот архив делаем ему иконку в виде нашей фотографии, а также с помощью специального символа меняем местами gpj и .exe. Следующим шагом придумали слово, которое маскирует exe.