**Тема: “WinLocker & KeyLogger”.**

**Проект будет разделен на две части:**

**Часть 1:** Winlocker

**Часть 2:** Keylogger.

**Часть 1: Winlocker**

**Цель разработки:**

Необходимо разработать вредоносное программное обеспечение, которое будет иметь возможность блокировать системные процессы, они же в свою очередь будут блокировать доступ пользователю к своей операционной системе.

**Основания для разработки:**

Поиск возможных дыр в безопасности системы

**Основные функции WinLocker:**

1. Автозапуск WinLocker.

2. Блокировка доступа системных шорт катов (сочетаний клавиш по типу alt +f4, alt+tab и т.д).

3. Вывод окна вредоносного ПО поверх других окон и развертывание на весь экран.

4. Возможность убрать окно с WinLocker с помощью разблокировки с паролем.

5. Выключение системы / компьютера при неудачных 3-х попытках ввода пароля для разблокировки.

6. Блокировка доступа к возможностям операционной системы.

**Требования к программе:**

1. Автозапуск вредоносного ПО

2. Блокировка доступа к возможностям контактирования с файлами системы

3. Блокировка системных шорт катов

**Задача**

1. Разработать вредоносную программу, которая будет затруднять работу с операционной системой.

**Принцип работы Winlocker:**

Вне зависимости от классификации и типов, винлокеры всегда выполняют одну и ту же функцию — блокирование доступа к операционной системе. Данное действие достигается блокированием доступа всей рабочей области экрана и частичной блокировкой устройств ввода (клавиатура, мышь).

**Конструкторские документы:**

YouTube  
GitHub  
ProgLib

**Технические отчеты:**

Советуем использовать программу только в научных целях, а не для личный выгоды.

**Технические условия:**

* Сервер на котором находятся данные KeyLogger’a
* ПК для разработки

**Роли при разработке**

**Иванов Артём** - тестировщик;

**Пахомов Григорий** - технический писатель;

**Поляков Алексей** - разработчик;

**Милошевич Никола** - руководитель проекта;

**Барченков Михаил** - исследователь ИБ.

**Среда разработки:**

1. Язык программирования Python

2. PyCharm  
3. Операционная система Windows

**Часть 2:** Keylogger

**Цель разработки:**

Необходимо разработать вредоносное программное обеспечение, которое будет регистрировать различные действия пользователя — нажатия клавиш на клавиатуре компьютера, движения и нажатия клавиш мыши и т.д. Собирая информацию, вредоносное ПО будет отправлять логи в Telegram-bot злоумышленника.

**Основные функции Keylogger:**

1. Автозапуск Keylogger.

2. Маскировка данного вредоносного ПО под обычный файл или процесс (например: различные браузеры, популярные программы).

3. Сохранение информации о действиях пользователя.

4. Автоматическая отправка логов в Telegram-bot злоумышленника.

**Требования к программе:**

1. Автозапуск вредоносного ПО

2. Считывание данных с клавиатуры

3. Отправления логов о действиях и нажатиях пользователя

**Задачи:**

1. Разработать вредоносную программу

2. Отслеживать действия сотрудников компании  
3. Отправка логов в текстовом виде в Telegram-bot.

**Принцип работы Keylogger:**

Keylogger Фиксирует нажатия клавиш на клавиатуре в различных приложениях и информацию, копируемую в буфер обмена. Позволяет перехватывать логины и пароли и отслеживать аккаунты сотрудника на «потенциально опасных» ресурсах. Программный модуль определяет пользователей, вводивших с клавиатуры пароли к зашифрованным документам.

ОСНОВНЫЕ ФУНКЦИИ:

1. Перехват нажатий клавиш.
2. Перехват нажатий функциональных клавиш.
3. Перехват текста из буфера обмена.

**Роли при разработке:**

**Иванов Артём** - тестировщик;

**Пахомов Григорий** - технический писатель;

**Поляков Алексей** - разработчик;

**Милошевич Никола** - руководитель проекта;

**Барченков Михаил** - исследователь ИБ.

**Среда разработки:**

1. Язык программирования Python

2. Операционная система Windows

3. PyCharm  
  
4. Язык программирования JavaScript