GitHub - Helixo32/NimBlackout: Kill AV/EDR leveraging BYOVD attack

By Helixo32

Archived: 2026-04-02 11:33:59 UTC

> **Note**: This project is for educational purposes only. The use of this code for any malicious activity is strictly prohibited. I am not responsible for any misuse of this software.

NimBlackout is an adaptation of the @Blackout project originally developed in C++ by @ZeroMemoryEx, which consists of removing AV/EDRs using the gmer (BYOVD) driver.

The main reason for this project was to understand how BYOVD attacks work, and then to provide a valid PoC developed in Nim.

All credit must goes to the original author @ZeroMemoryEx.

Usage

- Compilation
  - Linux

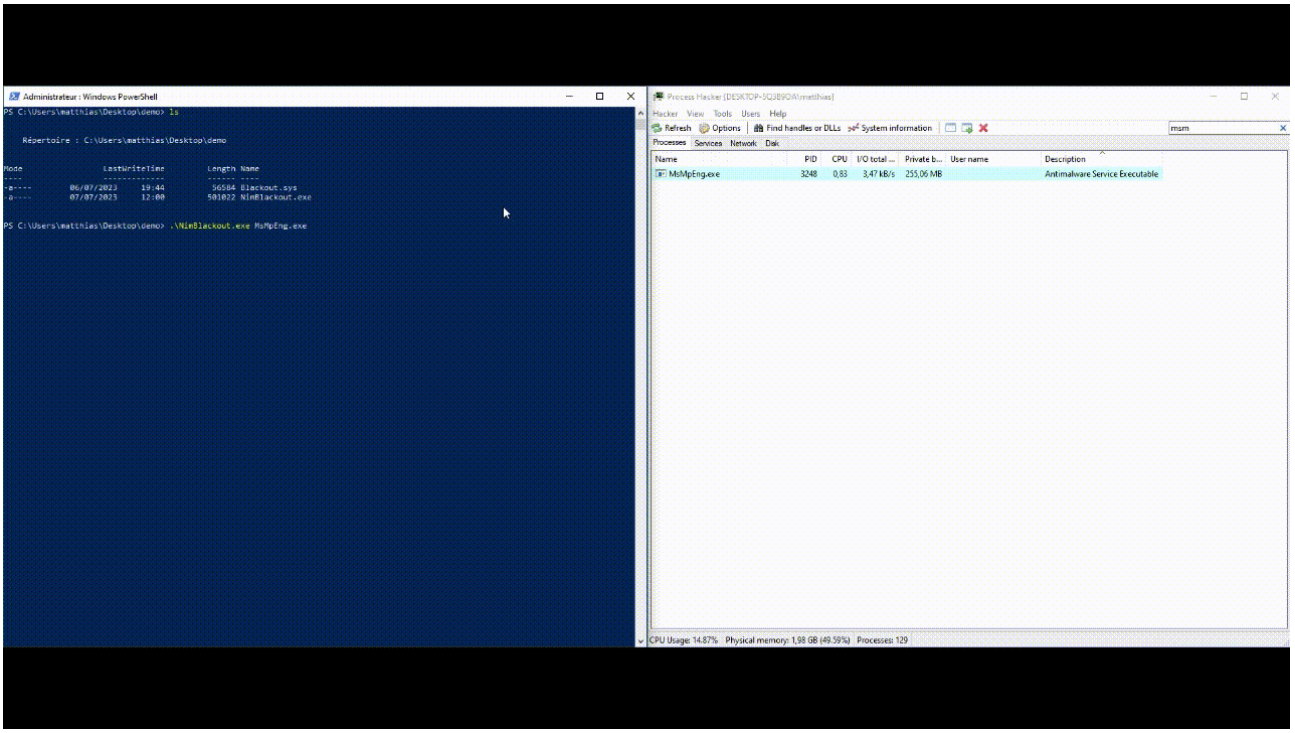
    ```
    nim --os:windows --cpu:amd64 --gcc.exe:x86_64-w64-mingw32-gcc --gcc.linkerexe:x86_64-w64-mingw32
    ```

  - Windows
- Put Blackout.sys driver into current directory
- Launch NimBlackout (with admin privileges)

  ```
  NimBlackout.exe <process name>
  ```

In order to prevent restarting process (like MsMpEng.exe), keep the program running.

Demo



Source: https://github.com/Helixo32/NimBlackout