

Forum:[Hack Forums](#)

Thread: [Kernel Karnage Series](#)

TheCyb3rAlpha - January 18, 2022, 11:14 pm

In this well explained series of blogpost (amazing blog btw: <https://blog.nviso.eu/>), you'll learn about AV/EDR detection & Kernel Callbacks hooking mechanism (including IRP Major Function Hooking) bypass technique that can render the EDRs useless. This blog series also focuses a little on Driver Signature Enhancement (DSE) and bypassing it.

Note: I'm not the author of this blog. Kudos to [@cerbersec](#) for this amazing blog series!

Spoiler ([Click to View](#))

[Kernel Karnage Part 1](#)

Covers looking at User vs Kernel Space, how EDRs interact with them and concept of kernel drivers and kernel callbacks and how they are used by security software

[Kernel Karnage Part 2 - Back to basics](#)

Covers Anatomy of a driver, its functions & their main responsibilities and IRP Major Function Hooking

[Kernel Karnage Part 3 - Challenge accepted](#)

Covers the combination of Evil Driver & Interceptor Driver to Disable Kernel Callbacks and also hook IRP dispatch routines

[Kernel Karnage Part 4 - Interceptormezzo](#)

Covers more details on Interceptor Driver

[Kernel Karnage Part 5 - I/O callbacks](#)

Covers upgrading Interceptor Driver to handle I/O between kernel driver and user mode application to hook image load callbacks

[Kernel Karnage Part 6 - Last call](#)

Covers object callbacks & bypassing AV/EDR using updated Interceptor driver

[Kernel Karnage Part 7 - Out of the lab and back to reality](#)

Covers the usage of Kernel Callback bypass technique to execute Cobalt Strike beacon

[Kernel Karnage Part 8 - Getting around Driver Signature Enhancement \(DSE\)](#)

Covers developing Beacon Object File (BOF) for Driver Signature Enforcement (DSE) bypass to load unsigned drivers and unload the AV/EDR registered register callbacks from Kernel