
KasperskyHook

Hook system calls on Windows by using Kaspersky's hypervisor

How does it work?

Kaspersky utilizes its hypervisor when hardware virtualization is supported for additional protection. It hooks system calls by changing `IA32_LSTAR` to point to its own syscall handler (which is basically a copy of `KiSystemCall64`) so it dispatches system calls to its own handlers (while doing initialization, it builds its own dispatch table).

This project loads `klhk.sys` (Kaspersky's hypervisor module) and a custom driver which interfaces with it to subvert the system and hook system calls.

Why did you write this?

While researching Kaspersky components, I thought it was an interesting idea to write a custom project that lets me hook system calls by using Kaspersky's hypervisor to take a closer look at what it is doing.

Build steps - how to use it

- Download Visual Studio 2019, WDK, clone this repository and build the solution.
- Make sure `KasperskyHook.sys` and `KasperskyHookLoader.exe` are in the same folder. Copy `klhk.sys` to `\Windows\System32\drivers`
- Execute `KasperskyHookLoader.exe` and have fun :D

Troubleshooting

If you followed the Build and Testing steps and `kaspersky::hvm_init()` returns `C00000A3` or `C000090B`, try following these steps:

- Make sure Virtualization (VT-x/AMD-v) is supported and enabled.
- Check if there are any other hypervisors conflicting with `klhk` (such as other AVs)
- Delete all KasperskyHook-related services, cleanup registry information and reboot

If it still doesn't work, consider using a newer version of `klhk.sys`. More information: <https://github.com/iPower/KasperskyHook>

MAKE SURE TO ENABLE TEST MODE TO TEST THIS PROJECT. IF YOU WISH TO USE IT OUTSIDE TEST MODE, USE YOUR CUSTOM DRIVER LOADER OR SIGN THE DRIVER.

NOTE: THIS ISN'T MEANT TO BE AN EASY-TO-PASTE-DETECTION-PROOF PROJECT. I JUST WROTE THIS FOR EDUCATIONAL PURPOSES SO I WON'T BE ADDING ANY HV-HARDENING OR ANTI-DETECTION CODE.

Demo

