Hardware ID

- Does R5AC have hardware fingerprinting capabilities?

Does R5AC have hardware fingerprinting capabilities?

Not directly, but Apex Legends itself additionally uses **Theia** for a second form of machine fingerprinting. It doesn't replace EAC's mechanisms for the same thing, but rather seems to work alongside it. As an additional vector, so to speak.

The game will build a string that seems to resemble a hardware ID. I haven't reconstructed it fully yet, which is why this page is to be considered work in progress.

I've seen routines in both apex legends itself, but also theia's runtime which seem to be responsible for doing stuff with hardware identification. It seems like theia's runtime is doing all the heavy lifting, as i was able to trace a lot of NtDeviceIoControlFile calls from some suspicious region in apex legends. Of course it was the theia runtime. It led me to multiple giant functions which used various IOCTL codes and addressed different devices. Name of the devices were encrypted using some inline transformation in the code. But it seems fairly trivial to decrypt.

When i'll have some free time again, i will verify which codes are actually really queried in a live system.