In the following analysis, I will point out a few key features of the Detekt security software, and how certain functions are implemented.

The section I would like to address is in the rules folder. Inside is a file finfisher.yar, which contains a series of signatures that a computer infected with the finfisher malware might match.

This file is separated into lists of filters, which each correspond to files an infected computer might contains. The first filter is for passwords, 14 different possible regular expressions for 14 different accounts FinFisher may have hacked into. The second filter is for screen recordings. In the attached paper "FinFisher: The Nexus of Security and Human Rights," I detailed how FinFisher stores screenshots as files with the format XXYTTTTTTTT. As you can see from Detekt, it searches the system for files in the same layout, as a signature of the malware attack. The third filter is for keyloggers, as FinFisher also installs keyloggers in a system. The fourth filter is for any potential mic recorders. FinFisher can covertly take command of the microphone on a computer, and saves the recordings in this format. The fifth filter is for skype recordings. Recording video conversations is one of the most heavily advertised features of FinSpy. Often, FinSpy was installed in internet cafes, monitoring customers communications to see if they spoke with anyone outside the country. The sixth filter is for the file described in the aforementioned paper, driverw.sys. This is one of the primary files by which FinSpy is propagated. The last few filters are different settings and possible versions of FinSpy being installed.

When Detekt runs, it scans the address space for any of these possible rules, as they are hallmark signs of a FinSpy infection. It then performs a scan of the current memory being used by a program called volatility, whose job it is to extract digital artifacts from volatile memory. From these two sources, Detekt is able to verify the presence of FinSpy.

Finally, I have also attached two Snort rules from EmergingThreats.net. They search the computers packet stream for a particular byte signature that is unique to FinSpy. By running these rules, one should be able to tell if your computer is infected.