Overview

This project proposes an idea that utilizes machine learning and databases to collect information on virus patterns to actively prevent them from infecting servers and computers. Machine learning is an integral part of this project. The program would analyse virus behaviours, user browsing patterns, computer system statuses, and the impact that a virus has on an infected computer. The program would run a scan of the system before and after virus attacks, and determine the impact that said virus had on the computer or server. For example, settings could be changed, registries may have been edited or files could have been deleted, all of which the program’s aim is to pick up and learn from. With enough data, the program would eventually be able to prevent the virus from being able to attack systems again and evolve as the virus does to keep up with it, something that current antiviruses lack.

With that in mind, the proposal is an automated system that prevents virus attacks. To eliminate a constant need for human interaction and humans to update their own knowledge of viruses and how to counter them, an advanced AI is required. In a controlled environment, viruses could be injected into a machine over and over, and leave the AI to figure out how it works, what it does, and how to prevent it from happening.

This idea stems from the existence of ethical hackers, or “white hat hackers”. These are hackers who work for genuine companies that send their program to the hacker, who then tries to hack into it, report on their success and explain the method they used so that the company can strengthen their defense. While viruses are slightly different in nature, the same hacking method where a human breaks into a defence is similar nonetheless. However, the biggest and most important thing to note is that while hacking methods can change, a virus is ever-evolving, with some of them capable of self mutation to evolve past antiviruses, and humans would only be able to notice the difference when they detect that a virus has infected the system through an antivirus wall. As a result, an AI would be more suitable for the task, to be able to take note of any changes a virus could make during every attack and be able to modify itself to continue protecting the system from ever being successfully attacked.

While the notion of a machine learning antiviruses isn’t completely unique, there are currently no antiviruses that present evolving AI as an option. Two companies are currently developing such an idea though, with the first being Kaspersky and the other being a new antivirus called CrowdStrike Falcon Prevent. Both of them aim to develop a machine that is capable of distinguishing words from incomprehensible strings of letters to defend against attacks. The proposed project however, is designed to read a virus code and learn how it works, defending it from the inside in a sense. Rather than trying to constantly “overkill” and strengthen defences endlessly, the program would be designed to learn how certain viruses evolve and adapt faster than it can mutate to defend it.