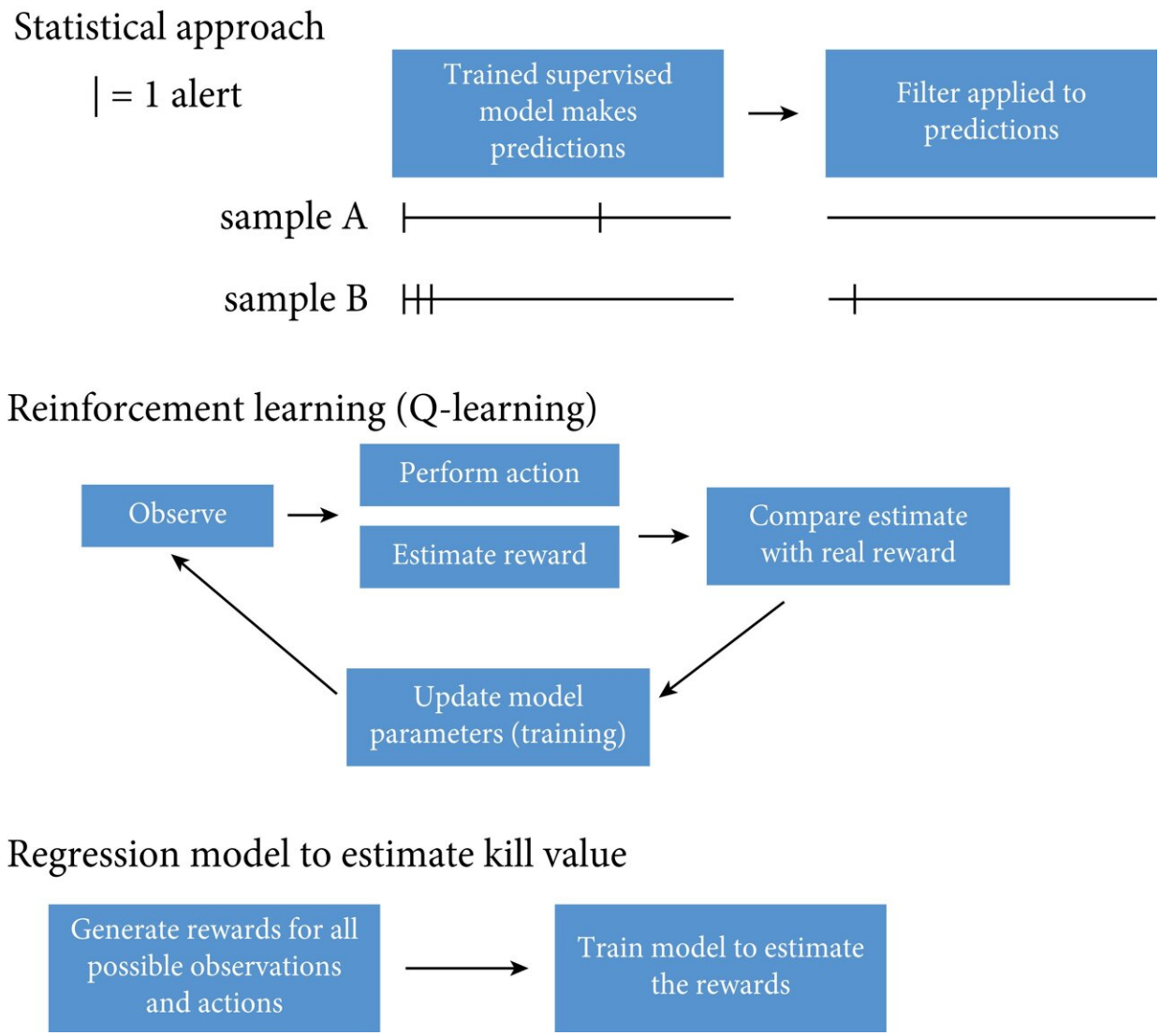
New method to kill cyberattacks in less than a second

May 20 2022



High-level depiction of three approaches taken. Credit: *Security and Communication Networks* (2021). DOI: 10.1155/2021/8933681

A new method that could automatically detect and kill cyberattacks on our laptops, computers and smart devices in under a second has been created by researchers at Cardiff University.

Using artificial intelligence in a completely novel way, the method has been shown to successfully prevent up to 92 percent of files on a computer from being corrupted, with it taking just 0.3 seconds on average for a piece of malware to be wiped out.

Publishing their findings in the journal *Security and Communications Networks*, the team say this is the first demonstration of a method that can both detect and kill malicious software in real-time, which could transform approaches to modern cybersecurity and avoid instances such as the recent WannaCry cyberattack that hit the NHS in 2017.

Using advances in artificial intelligence and machine learning, the new approach, developed in collaboration with Airbus, is based on monitoring and predicting the behavior of malware as opposed to more traditional antivirus approaches that analyze what a piece of malware looks like.

"Traditional antivirus software will look at the code structure of a piece of malware and say 'yeah, that looks familiar'," co-author of the study Professor Pete Burnap explains.

"But the problem is malware authors will just chop and change the code, so the next day the code looks different and is not detected by the antivirus software. We want to know how a piece of malware behaves so once it starts attacking a system, like opening a port, creating a process or downloading some data in a particular order, it will leave a fingerprint behind which we can then use to build up a behavioral profile."

By training computers to run simulations on specific pieces of malware, it is possible to make a very quick prediction in less than a second of how the malware will behave further down the line.

Once a piece of software is flagged as malicious the next stage is to wipe it out, which is where the new research comes into play.

"Once a threat is detected, due to the fast-acting nature of some destructive malware, it is vital to have automated actions to support these detections," continued Professor Burnap.

"We were motivated to undertake this work as there was nothing available that could do this kind of automated detecting and killing on a user's machine in real-time."

Existing products, known as endpoint detection and response (EDR), are used to protect end-user devices such as desktops, laptops, and mobile devices and are designed to quickly detect, analyze, block, and contain attacks that are in progress.

The main problem with these products is that the collected data needs to be sent to administrators in order for a response to be implemented, by which time a piece of malware may already have caused damage.

To test the new detection method, the team set up a virtual computing environment to represent a group of commonly used laptops, each running up to 35 applications at the same time to simulate normal behavior.

The AI-based detection method was then tested using thousands of samples of malware.

Lead author of the study Matilda Rhode, now Head of Innovation and

Scouting at Airbus, said: "While we still have some way to go in terms of improving the accuracy of this system before it could be implemented, this is an important step towards an automated real-time detection system that would not only benefit our laptops and computers, but also our smart speakers, thermostats, cars and refrigerators as the 'Internet of Things' becomes more prevalent."

More information: Matilda Rhode et al, Real-Time Malware Process Detection and Automated Process Killing, *Security and Communication Networks* (2021). DOI: 10.1155/2021/8933681

Provided by Cardiff University