- Computer viruses / Artificial Intelligence (AI)

Detecting and analysing unknown malware by using AI

The Straits Times · 25 Jul 2022 · B3 · Lim Min Zhang

While commercial anti-virus software can detect known malware, unknown malware engineered by sophisticated attackers, such as state-sponsored ones, could evade such detection.

Traditional anti-virus solutions use databases of known malware signatures to identify and deal with it. But signatures are not available for unknown malware.

To solve this problem, DSO National Laboratories' engineers are applying a technique known as behavioural analysis, powered by artificial intelligence (AI), to detect abnormal behaviours in an organisation's computer systems.

This method is based on the knowledge that malware would have to interact with the system to achieve its goals, such as stealing information.

"Such behavioural deviations provide us a way to detect unknown malware," said Dr Teo Hong Siang, 50, who is a principal cyber-security researcher at DSO.

This system is being piloted across government agencies.

AI is being used not just in detection, but also in analysing malware to identify its capabilities.

Dr Khoo Wei Ming, 44, who is also a DSO principal cyber-security researcher, said going through hundreds of pages of code in a typical malware sample is a tedious and labour-intensive process that can take days or weeks.

The team developed a codematcher to significantly reduce the amount of code that needs to be analysed manually. This is based on the insight that programmers, including malware authors, reuse and copy code.

Testing this method on a malware program called PingPull, the DSO team reduced the code that needs to be analysed by 77 per cent. This reduction allows analysts to analyse the malware with much less effort, said Dr Khoo.