MACHINE LEARNING AND CYBERSECURITY

Traditional security systems are failing because they are passive, and a small code change can lead to safer networks being attacked. The problem is that most security systems are based primarily on static knowledge.

The fundamental principle of machine learning is to recognize patterns that emerge from past experiences and make predictions based on them. This means reacting to a new invisible threat, based on a known data set, from the program learns and develops the ability to react to unknown new data.

However, any quality solution has to incorporate predictive modeling with expert input and data mining.

REAL-WORLD APPLICATION OF MACHINE LEARNING IN CYBER SECURITY

The most common and serious network security threats are brute-force attacks, intrusions, and DDoS attacks.

In a research project task was divided into three steps:

1) Detect network traffic flow that can compromise the botnet command and control infrastructure
2) Group the traffic flows from the same botnet by correlating them with each other
3) Identify the command and control host, which should help to identify the attack host

Machine learning techniques were used to identify the command and control traffic of IRC (Internet Relay Chat) based botnets.

The results of the research indicated that machine learning techniques can indeed distinguish the subtle differences in the IRC flows. However, one of the challenges in using this technique is the availability of an accurately labelled sample data set for training and testing.

CONCLUSION

Traditional cybersecurity applications rely on fixed rules, signatures, and algorithms, and can only act on the "knowledge" that has been provided to them. In the case of a new threat, previously undetected, these applications may not be able to locate it. However, machine learning applications are based on "learning" algorithms, which check an increasing data set.