Machine learning algorithm for advanced persistent threat detection.

Vincent Omollo and Silvance Abeka,
Kisii University, Kenya.
Jaramogi Oginga Odinga University of Science and Technology, Kenya.

Networked computer syster:ns are increasingly being employed to run critical infrastructural activities by both private companies and governments. Advanced persistent threats have emerged as serious security threats to these networks due to their level of sophistication and multiple attack vectors. Conventional countermeasures against these network threats have been antivirus, anti-malware, firewalls, intrusion detection systems, intrusion prevention systems and sandboxing. However, these techniques are ineffective against advanced persistent threats since the attackers employ a number of evasion techniques such as code obfuscation and encryption. In addition, these technologies are rarely monitored or updated, hence lulling end-user enterprises into a false sense of security. The signature based scanning utilized in some of these technologies is unable of detecting new and sophisticated malware. Sandboxes on their part, a number of malware deploy sandbox detection techniques that help them detect when they are being analyzed and evade the sandbox by hiding their malicious behavior. Due to these shortfalls, researchers have proposed machine learning, deep neural networks, and data mining using misuse detection and anomaly detection as possible threat detection strategies. Unfortunately, machine learning and deep neural networks are susceptible to evasion attacks using adversarial examples that involve small changes to the input data that cause misclassification at test time. Misuse detection is unable to discover attacks whose instances have not yet been observed while anomaly detection can generate false positives due to previously unseen and yet legitimate system behaviors being recognized as anomalies, and hence flagged as potential intrusions. The aim of this paper will be therefore to implement an enhanced algorithm for intrusion detection using machine learning to curb the rising number of advanced persistent threats.

Keywords: Intrusion detection; machine learning; APT; malware.