Singapore Cybersecurity Consortium
Anchored at NUS | Computing

Detecting Script-Based malware using Machine Learning

Ravikant TIWARI, Security Researcher

Sanjeev SOLANKI, Senior Researcher

Acronis Asia Research & Development Centre

ABSTRACT

Malicious scripts share a large chunk of threat landscape and poses serious threat to online users and endpoints. It manifests in all sorts of attack scenarios ranging from Exploits, APTs, Ransomwares, Trojan downloader, Remote Access Kits and many more. Antivirus software have hard time dealing with this threat due to missing structured file format like in case of PE, ELF, PDF, DOC etc. Scripts are plain text files and therefore it's hard to draw a fine line between malicious and non-malicious file for pre-filtering. This causes rules and signatures to be very strict and results in very ineffective detections.

We propose a machine learning based solutions for scripts-based malware detection which will be part of our Acronis cyber security solution. The MIME type text files will be pre-processed to filter out scripts and then multi-dimensional features will be extracted based on file geometry and content to classify it as malware or benign.