Automatic malware detection given changes to file systems

Saketh Ayyagari
Science & Engineering
Manalapan High School
Englishtown, NJ
425sayyagari@frhsd.com

Sanath Kumar
Commvault
Tinton Falls, NJ
skumar@commvault.com

Abstract

When malware gains access to an operating system, it can detrimentally affect it by altering a user's files in different directories. By monitoring whether the number of changes that occur in a specific time interval deviate from user patterns, one can infer the presence of a potential anomaly or piece of malware, prompting a user to take action against it. To automate this detection process, timestamps of directory metadata were collected in a specific time interval and compiled into a Structured Query Language (SQL) database. Once collected, the database is analyzed by an anomaly detection script, which utilizes a statistical model to return potential anomalies by detecting deviations from regular user patterns. Once these potential anomalies are flagged, they are compared with other timestamps to ensure those flagged are neither caused by user or regularly-scheduled patterns.

Index Terms

malware detection, SQL, intenship, Commvault, directory metadata, traffic analysis, deviations, anomalies