A Framework for Effective Ransomware Detection and Mitigation

Song, Eric (School: Yorktown High School)

Ransomware attacks render data unusable and demand a ransom in order to restore data integrity. These attacks destroy billions of dollars every year in lost data and productivity at the individual, industrial, and national security levels. This research aims to mitigate the threat of ransomware through an efficient detection system. By intercepting the malware during the file encryption process and extracting the encryption key from memory dumps, restoring data can be done without payment of ransom. The malware is intercepted by file and resource monitoring to detect anomalous behavior. Once intercepted, the system dumps the program's memory to a file that can then be analyzed for ransomware behavior and/or encryption keys, preventing data loss or lost productivity for extended periods of time. The system aims to reduce the time needed for technical teams to restore full access to a clean and secure computer network. The system designed was partially effective, doing well in detecting simple ransomware samples, however falling short with more sophisticated samples. That being said, the detection system used considerably less rules and, as a result, was less resource-intensive and more compatible with a variety of operating systems when compared to commercial systems today. In the future, more research is needed to create better ransomware detection techniques since the rule-based detection system used is limited in detecting novel ransomware samples.

Awards Won:

Second Award of $2,000