Lane Gramling
EECS 700
Reading 8

Summary - CryptoLock (and Drop It)

This paper outlines the design, function, and performance of a ransomware detection software built by the authors, dubbed CryptoLock. CryptoLock operates alongside traditional antivirus software, acting as a filesystem filter. From this source, CryptoLock monitors disk operations and detects potential ransomware by listening for suspicious operation patterns in file type changes, similarity measurements, and changes in a file's Shannon entropy score. These patterns used in concert are capable of early detection on the massive amounts of file encryption carried out by ransomware. This deviates from the approach of most current intrusion detection systems and antivirus software, which rely on matching flags and behavioral signatures of previously known malware.

Contributions

A major contribution of the paper is a theorization of how data is quantitatively affected by ransomware. Proposed are three major classes of behaviors, which if observed in concert are likely to indicate a ransomware beginning its siege. The first class is file type changes. When abnormally large amounts of varying file types are being changed to a single file type, this is likely to indicate that a malicious piece of software is attempting to obfuscate files on the machine. The second is to determine a similarity measurement for files before and after changes. Low scores are likely to indicate that the data has been transformed into something unrecognizable. The last major class is the Shannon entropy measurement of a file. The authors note that consistently high entropy output is a sign that files are being encrypted into unrecognizable data.

The next major contribution of the paper is the authors' analysis of their proposed system's performance with their experimental implementation. Their performance results show a high accuracy in true positives and a low probability for false positives. Additionally, respectable early detection times are seen, with a median of 10 files affected before the ransomware is caught.

Limitations

Despite the high accuracy of true positives, there was lacking elaboration in the software's performance in other detection categories, only providing that false positives are unlikely to trigger from operations carried out by regular user interaction. Additionally, the authors state that there is millisecond order latency added to disk operations, most noticeably in write and rename operations. The paper also falls into the same trap as the last paper by asserting VirusTotal as their fundamental truth for malware information. Perhaps most glaring is that the final say of whether to stop a potential ransomware attack is left to the jurisdiction of the user, leaving the user (who left themself vulnerable to attack) in charge of judging whether or not to trust the suspicious application.

Future Work

A good foundation is laid in this paper for further inquiry into observing structural changes in data for early detection of ransomware activity. As suggested by the authors, there is plenty of room for further performance improvements with a better optimized implementation of their design. Additionally, decisions can be made to monitor different parts of the filesystem than just the user's personal files. For example, The CryptoLock implementation in the paper does not monitor access to program files or operating system files, presumably in the interest of performance. Although operating system files are unlikely to be a target, it could provide added security to include program files under the umbrella of CyptoLock's protection, assuming a further optimized implementation would provide fast enough performance for this to be feasible.