# CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data

Paper Summary

Ruturaj Kiran Vaidya
University of Kansas

## 1 Summary

This paper proposes 'Cryptodrop' that monitors and detects the changes in the user data and alerts the user if the suspicious activity is detected. 'Cryptodrop' is effective when user's antimalware system fails to detect and block the threat. Authors characterized the ransomwares in three major classes, based on their operation. "Through extensive analysis, authors identified three primary and two secondary indicators, which are suited to detect malicious file changes"[1]. The primary indicators are - file type changes (where, they keep track of file types before and after the file is written), similarity measurement (they calculate similarity score after changes using 'sdhash' function) and Shannon entropy (ransomware attacks result in high entropy, thus they detect malicious activity by calculating entropy data). "When all three have manifested (i.e. union), a ransomware file transformation has likely occurred"[1]. "This union (which is crucial for the early detection) assists 'Cryptodrop' in reliably detecting file transformation, with few false positives"[1]. Detection and dile type funneling helps to fill the gaps left by primary indicators. "CryptoDrop focuses on detecting ransomware through monitoring the real-time change of user data"[1]. It develops a reputation score, by tracking the indicators, and process monitoring. Authors claimed that it demonstrated 100% true positive rate, also it remains robust, despite of the differences between the ransomware families.

## 2 Contribution

The authors presents 'Cryptodrop', which monitors changes in user data and alerts the user if the suspicious activity is detected, unlike previously proposed tools, which attempts to identify the ransomware (and not the transformation). It reduces the need of paying ransom by avoiding or blocking the ransomwares in the first place.

## 3 Strengths

'Cryptodrop' represented 100% true positive rate (over 492 ransomware samples), with only 0.2% file lost. Also, despite of the significant differences between ransomware families, it stays robust. I liked that they classified ransomwares depends on their operating (they also find that how these classes differ in their order of encryption).

## 4 Limitations

The important limitation is the performance overhead. Authors claimed that, their research version of 'Cryptodrop' tool is not optimized and "high latency of read and write operations often manifests during measurement"[1]. Also class 'B' samples has highest number of file lost (in case of ctb-locker). Also ordering of files attacked influences speed and incurs an overhead.

## 5 Future Work

I think 'dynamic scoring' without affecting false positives can be a future work, as suggested by authors. Hence, ultimately decreasing overhead or creating a performance optimized tool similar to 'Cryptodrop' (or modifying 'Cryptodrop' itself) can be a future work.

# References

[1] N. Scaife and H. Carter and P. Traynor and K. R. B. Butler *CryptoLock (and Drop It): Stopping Ransomware Attacks on User Data*, IEEE, (2016)