UNVEIL: A Large-Scale, Automated Approach to Detecting Ransomware

Jeff Malavasi
Dept. of Computing Security
Rochester Institute of Technology
Email: jm3378@rit.edu

I. Review

The authors of the paper propose a novel malware detection system that specifically attempts to detect ransomware. Previously, researchers have successfully created general malware detectors, but none have been targeted at a specific malware family. Since ransomware has the ability to both compromise a system and produce revenue for the bad actor, the prevalence of attacks has grown immensely. In this paper, the authors create and validate a system called UNVEIL that uses dynamic analysis to detect both file and screen locker ransomware [1].

File locking ransomware is a type of malware that targets files stored on a users machine and either partially or fully compromises availability. In order to detect this type of ransomware, the authors created a Cuckoo Sandbox plugin that utilized custom Windows kernel drivers. They measured each I/O operation on the disk and logged the process name, file path, type, and other metadata about the operation. The researchers found that ransomware could be detected by measuring entropy as well as looking for repeated patterns of file operations [1]. Additionally, the researchers generated artificial user environments that were comprised of realistic documents, photos and file structures that would subvert any sandbox evasion techniques used by the ransomware [1].

Screen locking ransomware not only compromises the end user's files, but additionally locks system files preventing access to the computer in general. In order to detect for this, the researchers captured screenshots before and after the sandbox analysis and measured the structural similarity between the images. Additionally, they also used OCR techniques in order to attempt to identify ransom notes to help reduce false positives [1].

The researchers then validated their system by running both a proof of concept and large scale experiment. In the proof of concept, they utilized a labeled dataset of around 3,000 malicious samples as well as 149 benign samples. In this experiment, they achieved a detection rate of 96.3% with a 0% false positive rate [1]. Next, the researches tested the system against a larger, unlabeled dataset to prove if it would be capable of detecting zero-day malware. They utilized a much large dataset of 150,000 samples and UNVEIL labeled 13,637 samples as ransomware, again with a false positive rate of 0% [1].

The authors were able to successfully create a plugin for Cuckoo sandbox that was able to accurately detect and classify ransomware. Additionally, they were able to discover novel families much quicker than industry leaders such as VirusTotal. However, there were also a few limitations. For example, their extremely low false positive rate may be indicative of an unbalanced dataset, since they did not test many benign samples. Additionally, they noted a need for improvement on the text extraction system used to detect screen locking ransomware. Finally, the current system is unable to detect kernel based ransomware. Although the authors noted this is not common, as the user often has the necessary privileges to lock the system, I believe this will change as zero trust environments expand and less users are granted administrative privileges.

While the field has created many general malware detection systems, it is also important to created targeted systems that detect specific families. Often ransomware can go undetected because it has a similar behavior signature to compression or encryption software. The authors create a new system that improves our ability to detect ransomware. Future research will be needed to create more detectors for other malware families.

References

[1] A. Kharaz, S. Arshad, C. Mulliner, W. Robertson, and E. Kirda, "UNVEIL: A Large-Scale, automated approach to detecting ransomware," in *25th USENIX Security Symposium (USENIX Security 16)*. Austin, TX: USENIX Association, 2016, pp. 757–772. [Online]. Available: https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/kharaz