Abstract

Ransomware has become one of the main cyber-threats for mobile platforms and in particular for Android. The number of ransomware attacks are increasing exponentially, while even state of art approaches terribly fail to safeguard mobile devices. In this paper, DNA-Droid, a two layer detection framework is proposed. It benefits of a dynamic analysis layer as a complementary layer on top of a static analysis layer. The DNA-Droid utilizes novel features and deep neural network to achieve a set of features with high discriminative power between ransomware and benign samples. Moreover, Sequence Alignment techniques are employed to profile ransomware families. This helps in detecting ransomware activity in early stages before the infection happens. The DNA-Droid is tested against thousands of samples. The experimental results shows high precision and recall in detecting even unknown ransomware samples, while keeping the false negative rate below 1.5%.

Contributions

✓ Introduce novel features with high discriminative power; making the DNA-Droid capable of recognizing unknown ransomware samples.
✓ Investigate the performance of Deep Auto Encoder to reduce and learn new features.
✓ Utilize Binary and Multiple Sequence Alignment (MSA) techniques to analyze dynamic system call sequences.
✓ Release a publicly available fully automated Android sandbox that is able to report the sequence of API calls as a web service.

Conclusion

The experimental results show that the DNA-Droid is able to discriminate between ransomware and benign samples with high precision and that it outperforms state of the art approaches. It shows a high capability to detecting ransomware activity in early stages before the infection happens.