prevent zero-day attack. Similar to FireEye, it does not have the capability to dynamically analyze document contents.

4 Conclusion

We have reviewed the recent trends in Malware and the latest techniques used to infiltrate existing systems. We have also study on few examples of existing threat detection systems and the various methods used by these systems as well as their shortcoming. We hope that this paper can be used as a guide for future analysis on malware threat and design.

References

1. www.norsecorp.com
2. http://www.thestar.com.my/tech/tech-news/2017/03/10
3. https://www.symantec.com/
4. https://www.fireeye.com/
5. https://www.lastline.com/

