**REFERENCES**

[1] D. Sahoo, C. Liu, S.C.H. Hoi, “Malicious URL Detection using Machine

Learning: A Survey”. CoRR, abs/1701.07179, 2017.

[2] M. Khonji, Y. Iraqi, and A. Jones, “Phishing detection: a literature

survey,” IEEE Communications Surveys & Tutorials, vol. 15, no. 4, pp.

2091–2121, 2013.

[3] M. Cova, C. Kruegel, and G. Vigna, “Detection and analysis of drivebydownload

attacks and malicious javascript code,” in Proceedings of the

19th international conference on World wide web. ACM, 2010, pp. 281–

290.

[4] R. Heartfield and G. Loukas, “A taxonomy of attacks and a survey of

defence mechanisms for semantic social engineering attacks,” ACM

Computing Surveys (CSUR), vol. 48, no. 3, p. 37, 2015.

[5] Internet Security Threat Report (ISTR) 2019–Symantec.

https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-

2019-en.pdf [Last accessed 10/2019].

[6] S. Sheng, B. Wardman, G. Warner, L. F. Cranor, J. Hong, and C. Zhang,

“An empirical analysis of phishing blacklists,” in Proceedings of Sixth

Conference on Email and Anti-Spam (CEAS), 2009.

[7] C. Seifert, I. Welch, and P. Komisarczuk, “Identification of malicious

web pages with static heuristics,” in Telecommunication Networks and

Applications Conference, 2008. ATNAC 2008. Australasian. IEEE,

2008, pp. 91–96.

[8] S. Sinha, M. Bailey, and F. Jahanian, “Shades of grey: On the

effectiveness of reputation-based “blacklists”,” in Malicious and

Unwanted Software, 2008. MALWARE 2008. 3rd International

Conference on. IEEE, 2008, pp. 57–64.

[9] J. Ma, L. K. Saul, S. Savage, and G. M. Voelker, “Identifying suspicious

urls: an application of large-scale online learning,” in Proceedings of the

26th Annual International Conference on Machine Learning. ACM,

2009, pp. 681–688.

[10] B. Eshete, A. Villafiorita, and K. Weldemariam, “Binspect: Holistic

analysis and detection of malicious web pages,” in Security and Privacy

in Communication Networks. Springer, 2013, pp. 149–166.

[11] S. Purkait, “Phishing counter measures and their effectiveness– literature

review,” Information Management & Computer Security, vol. 20, no. 5,

pp. 382–420, 2012.

[12] Y. Tao, “Suspicious url and device detection by log mining,” Ph.D.

dissertation, Applied Sciences: School of Computing Science, 2014.

[13] G. Canfora, E. Medvet, F. Mercaldo, and C. A. Visaggio, “Detection of

malicious web pages using system calls sequences,” in Availability,

Reliability, and Security in Information Systems. Springer, 2014, pp.

226–238.

[14] Leo Breiman.: Random Forests. Machine Learning 45 (1), pp. 5- 32,

(2001).

[15] Thomas G. Dietterich. Ensemble Methods in Machine Learning.

International Workshop on Multiple Classifier Systems, pp 1-15,

Cagliari, Italy, 2000.

[16] Developer Information. https://www.phishtank.com/developer\_info.php.

[Last accessed 11/2019].

[17] URLhaus Database Dump. https://urlhaus.abuse.ch/downloads/csv/.

[Ngày truy nhập 11/2019].

[18] Dataset URL. http://downloads.majestic.com/majestic\_million.csv. [Last

accessed 10/2019].

[19] Malicious\_n\_Non-MaliciousURL. https://www.kaggle.com/antonyj453/

urldataset#data.csv. [Last accessed 11/2019].

[20] chrome.zip.

https://drive.google.com/file/d/13G\_Ndr4hMFx\_qWyTEjHuOyJmHFW

D0Gud/view?fbclid=IwAR0SLVCrvjHHGmoHZH97nXN3Bm-

DMY7jG4SOsKZYLAZjTFgeoJADfli64-g. [Last accessed 12/2019].