IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

Cyber Guardian : Intelligent Threat Surveillance

Aditi. H. R.[1], Anusha Bhaskar D[2], Priyanka. H. V.[3]
Undergraduate Students, Department of Information Science and Engineering[1,2]
Assistant Professor, Department of Information Science and Engineering[2]
Global Academy of Technology, Bangalore, India

Abstract: *Advanced persistent threats (APTs) are cyberattacking that use covert strategies to target specific groups. As a result of the rapid growth of computing technology and the widespread connectivity of devices, there has been a boom in data transfer across networks. Because APTs' attack tactics are always changing, it can be difficult to detect them. This has led cybersecurity experts to develop creative solutions. We found gaps in the research on APT detection by doing a systematic literature review (SLR) covering the years 2012 to 2022 and finding 75 studies related to computer, mobile, and Internet of Things technologies. The most sophisticated cyberattack, known as an advanced persistent threat, involves malevolent individuals breaking into a network without authorization and staying hidden for an extended period. Advancement persistent threat attacks and organizational threats are becoming more frequent. Machine learning is one technique used to detect attacks by sophisticated persistent threats. The need for improved detection methods is highlighted by our findings, and we offer suggestions to guide the creation of early APT detection models and progress in cybersecurity. We propose a conceptual model known as Cyber Guardian that uses Random Forest classifier and attention techniques to create a self-translation machine through an encoder-decoder framework. These advanced attention algorithms are intended to improve the machine's capacity to examine and decipher intricate patterns found in HTTP requests, enhancing APT detection capabilities, and providing cybersecurity experts with cutting-edge instruments to proactively detect and neutralize new threats in real-time. This all-encompassing strategy is a major advancement in the ongoing fight against Advanced Persistent Threats (APTs) and emphasizes how crucial it is for the cybersecurity community to continuously innovate and collaborate in order to remain ahead of changing cyberthreats.*

Keywords: web application attack, advanced persistent threat, APT malware, Network traffic, Cyber Security, Cyberthreats.

REFERENCES

[1]. Salim DT, Singh MM, Keikhosrokiani P. A systematic literature review for APT detection and effective cyber situational awareness (ECSA) conceptual model. Heliyon. 2023 Jun 16.
[2]. Talib MA, Nasir Q, Nassif AB, Mokhamed T, Ahmed N, Mahfood B. APT beaconing detection: A systematic review. Computers & Security. 2022 Aug 21:102875.
[3]. Zou Q, Sun X, Liu P, Singhal A. An approach for detection of advanced persistent threat attacks. Computer. 2020 Dec 1;53(12):92-6.
[4]. Hasan MM, Islam MU, Uddin J. Advanced Persistent Threat Identification with Boosting and Explainable AI. SN Computer Science. 2023 Mar 20;4(3):271.
[5]. Al-Saraireh J. A novel approach for detecting advanced persistent threats. Egyptian Informatics Journal. 2022 Dec 1;23(4):45-55.
[6]. Liu T, Qi Y, Shi L, Yan J. Locate-Then-Detect: Real-time Web Attack Detection via Attention-based Deep Neural Networks. InIJCAI 2019 Aug 10 (pp. 4725-4731).
[7]. Yan L, Xiong J. Web-APT-Detect: a framework for web-based advanced persistent threat detection using self-translation machine with attention. IEEE Letters of the Computer Society. 2020 Jun 1;3(2):66-9.
[8]. He D, Gu H, Zhu S, Chan S, Guizani M. A comprehensive detection method for the lateral movement stage of apt attacks. IEEE Internet of Things Journal. 2023 Oct 6.

IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.53
Volume 4, Issue 1, February 2024

[9]. Do Xuan C, Dao MH. A novel approach for APT attack detection based on combined deep learning model. Neural Computing and Applications. 2021 Oct;33:13251-64.

[10]. Zhao G, Xu K, Xu L, Wu B. Detecting APT malware infections based on malicious DNS and traffic analysis. IEEE access. 2015 Jul 20;3:1132-42.

[11]. Chu WL, Lin CJ, Chang KN. Detection and classification of advanced persistent threats and attacks using the support vector machine. Applied Sciences. 2019 Oct 28;9(21):4579.

[12]. Xiong C, Zhu T, Dong W, Ruan L, Yang R, Cheng Y, Chen Y, Cheng S, Chen X. CONAN: A practical real-time APT detection system with high accuracy and efficiency. IEEE Transactions on Dependable and Secure Computing. 2020 Feb 3;19(1):551-65..

[13]. J. Straub, "Modeling attack, defense and threat trees and the cyber kill chain, att&ck and stride frameworks as blackboard architecture networks," in 2020 IEEE International Conference on Smart Cloud (SmartCloud). IEEE, 2020, pp. 148–153.

[14]. W. Tian, M. Du, X. Ji, G. Liu, Y. Dai, and Z. Han, "Honeypot detection strategy against advanced persistent threats in industrial internet of things: a prospect theoretic game," IEEE Internet of Things Journal, vol. 8, no. 24, pp. 17372–17381, 2021.

[15]. M. Tatam, B. Shanmugam, S. Azam, and K. Kannoorpatti, "A review of threat modelling approaches for apt-style attacks," Heliyon, vol. 7, no. 1, 2021.

[16]. Wang BX, Chen JL, Yu CL. Cyber security threat intelligence monitoring and classification. In2021 IEEE International Conference on Intelligence and Security Informatics (ISI) 2021 Nov 2 (pp. 1-3). IEEE.

[17]. J. Straub, "Modeling attack, defense and threat trees and the cyber kill chain, att&ck and stride frameworks as blackboard architecture networks," in 2020 IEEE International Conference on Smart Cloud (SmartCloud). IEEE, 2020, pp. 148–153.

[18]. Jiazhong Lu, Chen K, Zhuo Z, Zhang XS (2019) A temporal correlation and traffic analysis approach for APT attacks detec tion. Clust Comput 22:7347–7358

[19]. U. Noor, A machine learning framework for investigating data breaches based on semantic analysis of adversary's attack patterns in threat intelligence repositories, Future Generat. Comput. Syst. 95 (2019) 467–487.

[20]. Yan G, Li Q, Guo D, Meng X. Discovering suspicious APT behaviors by analyzing DNS activities. Sensors. 2020 Jan 28;20(3):731.

[21]. Al-Mohannadi H, Awan I, Al Hamar J, Al Hamar Y, Shah M, Musa A. Understanding awareness of cyber security threat among IT employees. In2018 6th international conference on future internet of things and cloud workshops (ficloudw) 2018 Aug 6 (pp. 188192). IEEE.

[22]. Abrahams TO, Ewuga SK, Dawodu SO, Adegbite AO, Hassan AO. A Review Of Cybersecurity Strategies In Modern Organizations: Examining The Evolution And Effectiveness Of Cybersecurity Measures For Data Protection. Computer Science & IT Research Journal. 2024 Jan 9;5(1):1-25.