Inteligência Artificial na Cibersegurança: Deteção de Malware

Tomás Antunes Nº48511

Abril 2022

Resumo

Software malicioso, ou malware, é uma das maiores ameaças à cibersegurança. Os ataques informáticos são cada vez mais comuns, todos os dias são criados novos programas maliciosos, com o intuito de causar dano a alguém, a empresas ou até mesmo a governos. Este software malicioso pode danificar a máquina em que está hospedado, pode danificar ficheiros, roubar informações, remover permissões do utilizador ou até executar operações no dispositivo sem a autorização do utilizador. A utilização de várias técnicas de inteligência artificial, como por exemplo Deep Learning e Machine Learning, tem vindo a aumentar, sendo que estas diminuem o trabalho necessário do humano para defender a máquina, fazendo assim uma mais rápida e mais precisa deteção destes softwares maliciosos, podendo assim poupar tempo e dinheiro às entidades atacadas, e evitar danos aos sistemas informáticos.

O objetivo deste trabalho é explorar a utilização da inteligência artificial na cibersegurança, na área da deteção de malware, e como esta permite que a internet seja um local mais seguro.

1 Introdução

A tecnologia tem vindo a evoluir rapidamente ao longo dos anos, criando a imagem de que vivemos numa sociedade de informação. Estamos constantemente rodeados por tecnologia, que usamos no nosso dia-a-dia. Esta rápida evolução da tecnologia apresenta um grande desafio, que é defender esta nova tecnologia de cibercriminosos. A inteligência artificial pode ajudar neste desafio ao ajudar os operadores de segurança humanos a detetar software malicioso, e assim facilitar o trabalho dos mesmos, poupando tempo e poupando dinheiro. Assim, também a defesa destes sistemas será mais precisa e mais eficaz, pois os operadores sabem exatamente o que "atacar".

2 Assinatura de Deteção vs Inteligência Artificial

Antes da inteligência artificial entrar para a área da segurança, uma das técnicas usadas para detetar software malicioso, era a deteção com base em assinaturas. Este é um método lento, e pouco eficaz, pois é realizado por operadores humanos, que podem cometer erros. O processo de desenvolver uma assinatura de deteção muitas vezes demora semanas, ou seja, o software malicioso podia já ter cumprido a sua missão, e sistemas vitais poderiam estar comprometidos. Mesmo com uma assinatura desenvolvida o atacante apenas precisa de fazer pequenas mudanças no software para este ultrapassar esta. Com a inteligência artificial, não só é mais rápida e mais eficaz a deteção como mesmo que o atacante faça mudanças no código, esta o volte a detetar bastante rapidamente.

3 Limitações

Como qualquer outra tecnologia, a inteligência artificial também tem limitações. A deteção de malware é dividida em duas partes, estática e dinâmica, onde ocorre o mapeamento do código do software detetado, sendo a análise dinâmica melhor, comparada com a estática. Uma das limitações do processo dinâmico é por exemplo, algumas operações realizadas pelo utilizador podem parar este processo, fazendo com que este possa falhar algum ou alguns vírus que estejam ativos. Este processo também assume que o estado inicial do ficheiro nunca é alterado o que nem sempre é verdade, podendo assim deixar passar alterações feitas pelo próprio vírus, fazendo com que este tenha maior probabilidade de cumprir a sua missão sem ser detetado.

4 Conclusão

Concluindo, a cibersegurança é uma área que está cada vez mais a precisar de ferramentas mais rápidas e mais eficazes, devido à rápida evolução da tecnologia e cada vez haver mais ataques informáticos, e os mesmos sendo cada vez mais

sofisticados. A inteligência artificial é uma tecnologia em constante desenvolvimento e melhoria, e uma tecnologia bastante útil na área da cibersegurança. Esta promete ser mais eficaz e mais rápida que o operador humano, e assim poupar recursos e dinheiro aos que usufruírem da mesma, assegurando assim uma internet mais segura.

Referências

[1] Mahmoud Abdelsalam, Maanak Gupta, and Sudip Mittal. Artificial intelligence assisted malware analysis. In *Proceedings of the 2021 ACM Workshop on Secure and Trustworthy Cyber-Physical Systems*, pages 75–77, 2021.

[2] Hasan Alkahtani and Theyazn HH Aldhyani. Artificial intelligence algorithms for malware detection in android-operated mobile devices. *Sensors*, 22(6):2268, 2022.

[3] Md Jobair Hossain Faruk, Hossain Shahriar, Maria Valero, Farhat Lamia Barsha, Shahriar Sobhan, Md Abdullah Khan, Michael Whitman, Alfredo Cuzzocrea, Dan Lo, Akond Rahman, et al. Malware detection and prevention using artificial intelligence techniques. In *2021 IEEE International Conference on Big Data (Big Data)*, pages 5369–5377. IEEE, 2021.

[4] Jannatul Ferdaos, Chandani Vaya, Anchal Bhalla, Ami Tharayil, and May El Barachi. Smart malware detection: From signatures to artificial intelligence. In *2020 5th International Conference on Smart and Sustainable Technologies (SpliTech)*, pages 1–6. IEEE, 2020.

[5] Maanak Gupta, Sudip Mittal, and Mahmoud Abdelsalam. Ai assisted malware analysis: A course for next generation cybersecurity workforce. *arXiv preprint arXiv:2009.11101*, 2020.

[6] Li-Chin Huang, Chun-Hsien Chang, and Min-Shiang Hwang. Research on malware detection and classification based on artificial intelligence. *International Journal of Network Security*, 22(5):717–727, 2020.

[7] Antonio Libri, Andrea Bartolini, and Luca Benini. paella: Edge ai-based real-time malware detection in data centers. *IEEE Internet of Things Journal*, 7(10):9589–9599, 2020.

[8] Al-Ani Mustafa Majid, Ahmed Jamal Alshaibi, Evgeny Kostyuchenko, and Alexander Shelupanov. A review of artificial intelligence based malware detection using deep learning. *Materials Today: Proceedings*, 2021.

[9] Subash Poudyal and Dipankar Dasgupta. Ai-powered ransomware detection framework. In *2020 IEEE Symposium Series on Computational Intelligence (SSCI)*, pages 1154–1161. IEEE, 2020.

[10] Sherif Saad, William Briguglio, and Haytham Elmiligi. The curious case of machine learning in malware detection. *arXiv preprint arXiv:1905.07573*, 2019.

[11] James Scott. Signature based malware detection is dead. *Institute for Critical Infrastructure Technology*, 2017.

[12] R Vinayakumar, Mamoun Alazab, KP Soman, Prabaharan Poornachandran, and Sitalakshmi Venkatraman. Robust intelligent malware detection using deep learning. *IEEE Access*, 7:46717–46738, 2019.