ZHI WANG **Zhongguancun Laboratory** **Assistant Researcher**

wangzhi@zgclab.edu.cn · Haidian, Beijing · wzhi1997

EMPLOYMENT

2023 – Present **Zhongguancun Laboratory**, Assistant Researcher

EDUCATION

2017 – 2023 **UCAS / Institute of Information Engineering, CAS**, *Cyberspace Security*, Ph.D.
2013 – 2017 **Civil Aviation University of China**, *Information Security*, B.Eng.

RESEARCH INTERESTS

Cyber Attack and Defense AI-powered attack & defense, malware, botnets, anonymous networks
Intelligent Cognitive Security Cognitive data analysis

RESEARCH PROJECTS

- National Natural Science Foundation of China (NSFC), Principal Investigator
- National Science and Technology Major Project, Sub-project Leader
- National Laboratory Special Program, Key Member

PROFESSIONAL SERVICE

- Professional Member of the China Computer Federation (CCF); Executive Member of the CCF Technical Committee on Network and System Security; Executive Member of the CCF Technical Committee on Information Security; Member of the CCF Technical Committee on Computer Security
- Member of the Association for Computing Machinery (ACM), the Institute of Electrical and Electronics Engineers (IEEE), the China Cyber Security Society (CCSS), and the Chinese Association for Artificial Intelligence (CAAI)
- **Reviewer** TheWebConf2026 (WWW2026), IJCNN2026 (WCCI2026), IJCNN2025, ICASSP2025, Computers & Security, Cybersecurity, Blockchain, Journal of Cyber Security

PUBLICATIONS & PATENTS

Papers

- Zhe Huang, **Zhi Wang**, Chaoge Liu, Xiao Deng, Shengjia Chang, Mengyang Xu. Beyond the Blank Slate: Typed Operating System State for Cross-Session Consistency in LLM-Powered Honeypots. In 20th International Symposium on Research in Attacks, Intrusions and Defenses (**RAID**), Lancaster, UK. Springer, 2026.
- Zhe Huang, Chaoge Liu, **Zhi Wang**, Xiang Cui, Xiao Deng, Mengyang Xu. Package Hallucinations as Phantoms in Open-source Software Supply Chains: An Empirical Security Analysis. **ACM Transactions on Software Engineering and Methodology (TOSEM)**. 2026. DOI: 10.1145/3830237
- Yong Zhao, Ang Xia, Jie Yin, **Zhi Wang**, Yaqin Cao, Xiangyi Zeng, Yuling Liu. BASSET: Enhancing Binary Code Clone Searching through Multi-Level Hybrid Semantic Indexing. In 2025 55th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (**DSN**), Naples, Italy. IEEE, 2025: 47-60. DOI: 10.1109/DSN64029.2025.00020 (WOS:001589658100004)

- Chaoge Liu, **Zhi Wang**, Jie Yin, Yinsheng Liu, Kai Mao, Zhe Huang, Chumeng Deng. SCBot: Building Lightweight and Flexible C&C Based on Smart Contract. In 2025 IEEE International Conference on Acoustics, Speech and Signal Processing (**ICASSP**), Hyderabad, India. IEEE, 2025: 1-5. DOI: 10.1109/ICASSP49660.2025.10889707 (WOS:001611517600483)
- Xutong Wang, Jie Yin, Chaoge Liu, Chenchen Xu, Hao Huang, **Zhi Wang**, Fangjiao Zhang. A Survey of Backdoor Attacks and Defenses on Neural Networks. **Chinese Journal of Computers**, 2024, 47(8): 1713-1743. DOI: 10.11897/SP.J.1016.2024.01713 (in Chinese)
- Peng Liao, Binxing Fang, Chaoge Liu, **Zhi Wang**, Yuntao Zhang, Xiang Cui. Measurement and Detection Techniques for NFT Counterfeiting Fraud. **Chinese Journal of Computers**, 2024, 47(5): 1065-1081. DOI: 10.11897/SP.J.1016.2024.01065 (in Chinese)
- Peng Liao, Chaoge Liu, Jie Yin, **Zhi Wang**, and Xiang Cui. NFT Security Matrix: Towards Modeling NFT Ecosystem Threat. **Computer Modeling in Engineering & Sciences**. 2024, 139(3): 3255-3285. DOI:10.32604/cmes.2024.043855 (WOS:001166654400001)
- Cong Dong, Jiahai Yang, Song Liu, **Zhi Wang**, Yuling Liu, and Zhigang Lu. C-BEDIM and S-BEDIM: Lateral Movement Detection In Enterprise Network Through Behavior Deviation Measurement. **Computers & Security**. 2023: 103267. DOI: 10.1016/j.cose.2023.103267 (WOS:001006680400001)
- Yanhui Chen, Yun Feng, **Zhi Wang**, Jianjun Zhao, Chengchun Wang, and Qixu Liu. IMaler: An Adversarial Attack Framework to Obfuscate Malware Structure against DGCNN-based Classifier via Reinforcement Learning. In 2023 IEEE International Conference on Communications (**ICC**). IEEE, 2023: 790-796. DOI: 10.1109/ICC45041.2023.10279372 (WOS:001094862600127)
- Xutong Wang, Chaoge Liu, Xiaohui Hu, **Zhi Wang**, Jie Yin, and Xiang Cui. Make Data Reliable: An Explanation-powered Cleaning on Malware Dataset Against Backdoor Poisoning Attacks. In Annual Computer Security Applications Conference (**ACSAC**), ACM, 2022: 267 – 278. DOI: 10.1145/3564625.3564661 (WOS:001066271300020)
- **Zhi Wang**, Chaoge Liu, Xiang Cui, Jie Yin, Jiaxi Liu, Di Wu, and Qixu Liu. DeepC2: AI-Powered Covert Command and Control on OSNs. In 24th International Conference on Information and Communications Security (**ICICS**). Springer, Cham, 2022: 394-414. DOI: 10.1007/978-3-031-15777-6_22 (**Best Artifact Award**, WOS:000894187500022)
- **Zhi Wang**, Chaoge Liu, Xiang Cui, Jie Yin, and Xutong Wang. EvilModel 2.0: Bringing Neural Network Models into Malware Attacks. **Computers & Security**. 2022, 120: 102807. DOI: 10.1016/j.cose.2022.102807 (WOS:000841160900002)
- **Zhi Wang**, Jie Yin, Xiang Cui, Qixu Liu, Chaoge Liu, Xutong Wang. AI-Powered Cyber Threats: A Survey. **Journal of Cyber Security**, accepted. DOI: 10.19363/J.cnki.cn10-1380/tn.2024.04.09 (in Chinese)
- **Zhi Wang**, Chaoge Liu, and Xiang Cui. EvilModel: Hiding Malware Inside of Neural Network Models. In 2021 IEEE Symposium on Computers and Communications (**ISCC**). IEEE, 2021: 1-7. DOI: 10.1109/iscc53001.2021.9631425 (WOS:000936276000056)
- Fangjiao Zhang, Xiang Cui, **Zhi Wang**, Shaomian Chen, Qixu Liu, and Chaoge Liu. A Systematic Study of AI Applications in Cybersecurity Competitions. In 2020 IEEE 14th International Conference on Big Data Science and Engineering (**BigDataSE**). IEEE, 2020: 138-146. DOI: 10.1109/bigdatase50710.2020.00026 (WOS:000853058100019)
- Jie Yin, Xiang Cui, Chaoge Liu, Qixu Liu, Tao Cui, and **Zhi Wang**. CoinBot: A Covert Botnet in the Cryptocurrency Network. In 22nd International Conference on Information and Communications Security (**ICICS**). Springer, Cham, 2020: 107-125. DOI: 10.1007/978-3-030-61078-4_7 (WOS:001545251100007)
- Zihao Zhao, Qixu Liu, Tiantian Song, **Zhi Wang**, and Xianda Wu. WSLD: Detecting Unknown Webshell Using Fuzzy Matching and Deep Learning. In 21st International Conference on Information and Communications Security (**ICICS**). Springer, Cham, 2019: 725-745. DOI: 10.1007/978-3-030-41579-2_42 (WOS:000668350000042)
- **Zhi Wang**, Jinli Zhang, Qixu Liu, Xiang Cui, and Junwei Su. Practical Metrics for Evaluating Anonymous Networks. In 1st International Conference on Science of Cyber Security (**SciSec**). Springer, Cham, 2018: 3-18. DOI: 10.1007/978-3-030-03026-1_1 (WOS:000917197600001)

- Chaoge Liu, Xiang Cui, **Zhi Wang**, Xiaoxi Wang, Yun Feng, and Xiaoyun Li. MaliceScript: A Novel Browser-Based Intranet Threat. In 2018 IEEE 3rd International Conference on Data Science in Cyberspace (**DSC**). IEEE, 2018: 219-226. DOI: 10.1109/DSC.2018.00039 (WOS:001525065600030)
- Jingqiang Liu, Zihao Zhao, Xiang Cui, **Zhi Wang**, and Qixu Liu. A Novel Approach for Detecting Browser-Based Silent Miner. In 2018 IEEE 3rd International Conference on Data Science in Cyberspace (**DSC**). IEEE, 2018: 490-497. DOI: 10.1109/DSC.2018.00079 (WOS:001525065600070)
- Jinli Zhang, **Zhi Wang**. Poster: An Anonymity Metric of Anonymous Network. In 2018 IEEE Symposium on Security and Privacy (**S&P**). IEEE, 2018. (Poster)
- Junwei Su, Qixu Liu, **Zhi Wang**, and Xiaoyun Li. Poster: A Web Server Identified Model based on Mean Shift. In 2018 IEEE Symposium on Security and Privacy (**S&P**). IEEE, 2018. (Poster)
- Wei Jin, Hong Cui, **Zhi Wang**, Faqin Guo, Yiwen Wang, Shuai He. Detection and Control System for DDoS Attacks. **Cyberspace Security**, 2017, 8(Z3): 19-22. (in Chinese)

Patents

- Qixu Liu, Jianjun Zhao, Ru Tan, **Zhi Wang**, Feng Dai, Yaqin Cao, Xingchen Chen. A Threat Intelligence Sharing Method and Apparatus Compliant with Data Security Requirements. Chinese Invention Patent, ZL202210010348.3.

AWARDS & HONORS

Competitions & Awards

ICICS 2022	*Best Artifact Award*	Sep. 2022
DataCon, Network Traffic Analysis Track	*First Prize*	Oct. 2021
Coremail E-mail Security Analysis Contest	*Excellence Award*	Oct. 2020
National College Student Information Security Contest	*First Prize*	Aug. 2015

Honors

Outstanding CPC Member, Research Dept. 4, Zhongguancun Laboratory	Dec. 2023, 2024, 2025
Outstanding Team Member, National Cyber Defense Exercise, Zhongguancun Laboratory	May 2025
In-house Trainer, Institute of Information Engineering, CAS	Jul. 2021
Director's Excellence Award, Institute of Information Engineering, CAS	May 2021
Outstanding Communist Youth League Member, CAUC	May 2014, 2015, 2016

(Last updated: 2026-09-11)