王志 中国科学院大学　博士研究生

wangzhi@arkteam.net · (+86) 176-0066-5701 · wzhi1997

教育背景

2017 – 至今　**中国科学院信息工程研究所**, 网络空间安全, 硕博连读 (预计 *2023* 年夏季毕业)

2013 – 2017　**中国民航大学**, 信息安全, 学士

研究方向

网络攻防技术　AI 与网络攻防、僵尸网络、匿名网络

主要技能

- 掌握网络攻防、AI 与网络威胁原理，熟悉比特币网络、Web 追踪、邮件安全及常见密码算法等
- 编程语言: Python、Java、PHP、Vue、Shell、C#、C/C++

参与课题

- 高级威胁智能发现与溯源取证技术研究, 北京市科委
- 基于欺骗诱捕的高级威胁智能感知与溯源取证技术, 国家自然科学基金
- 中国科学院年度安全保障专项项目, 中国科学院
- 隐蔽信道构建技术, 中科院先导计划

科研经历

基于神经网络模型的恶意代码隐藏技术

预测人工智能在恶意载荷投递和定向攻击中的应用。本工作得到国内外科技媒体的广泛关注。

- 提出一种以神经网络模型为载体的恶意代码隐藏技术，能够在不影响模型性能的情况下，将恶意软件嵌入到模型内部
- 借助神经网络模型的单向性和 DeepLocker 思想，提出了一种隐蔽定向攻击模型，使恶意代码能准确有效地找到目标，而防御者无法提前找到攻击目标

关键词　*神经网络、AI 赋能的网络攻击、恶意代码隐写、隐蔽定向攻击*

基于图文语义理解的隐蔽命令控制技术

预测人工智能在恶意代码命令与控制中的应用。

- 针对传统 C&C 中控制端地址可被预测的问题，提出基于孪生神经网络的隐蔽寻址方案，使用图像特征作为控制端身份标识，达到被控端被逆向也不会泄露控制端地址的效果
- 针对在社交网络平台上发布 C&C 命令留下的异常内容问题，提出使用数据增强技术和哈希碰撞的方法，将命令隐藏在具备自然语义的内容中，消除异常

关键词　*神经网络、命令与控制、僵尸网络、社交网络*

基于域前置的隐蔽命令控制技术

利用域前置技术构建隐蔽 C&C 信道，借助公共服务平台构建信道恢复机制。

- 分析域前置技术原理，利用第三方云服务特性和 Tor Hidden Service 构建隐蔽 C&C 信道，复现该技术在 APT29 远控中的应用
- 研究基于 Web 2.0 公共服务的命令控制技术，使用社交网络、临时存储、信息映射等公共资源构建寻址信道，借助 DGA 技术实现信道恢复机制

关键词　*域前置、Tor、命令与控制、公共服务*

基于加密数字货币网络的隐蔽信道构建技术

利用数字加密货币网络构建抗封锁、防溯源的隐蔽信道。

- 研究加密数字货币及区块链技术，分析比特币交易的数据结构，利用比特币交易构建隐蔽信道
- 分析比特币交易依赖的椭圆曲线数字签名算法的安全问题，利用临时密钥重用攻击构建隐蔽信道

关键词 *比特币、区块链、命令与控制、椭圆曲线数字签名*

网络安全测试

针对目标系统进行 Web 安全、移动安全等网络安全测试。

- 针对大型企事业单位的信息系统进行网络安全测试，结合目标情况制定测试方案，发现 Web 安全、APP 安全和 VPN 安全等风险点，包括 SQL 注入、XSS、信息泄露、越权等漏洞
- 根据测试情况完成测试报告，结合漏洞详情提供修复方案，并跟踪漏洞修复

关键词 *Web 安全、移动安全、数据安全、渗透测试*

科研成果

论文

- **王志**, 尹捷, 崔翔等. 人工智能赋能网络威胁研究进展 [J]. 信息安全学报, 已采用. (CCF 中文-B)
- **Wang Z.**, Liu C., Cui X., et al. EvilModel 2.0: Bringing Neural Network Models into Malware Attacks[J]. Computers & Security. 2022, 120: 102807. DOI: 10.1016/j.cose.2022.102807 (CCF-B)
- **Wang Z.**, Liu C., Cui X. EvilModel: Hiding Malware Inside of Neural Network Models[C]. In 2021 IEEE Symposium on Computers and Communications (ISCC). IEEE, 2021: 1-7. DOI: 10.1109/iscc53001.2021.9631425 (CCF-C)
- **Wang Z.**, Liu C., Cui X., et al. DeepC2: AI-Powered Covert Command and Control on OSNs[C]. In 24th International Conference on Information and Communications Security (ICICS). Springer, Cham, 2022: 394-414. DOI: 10.1007/978-3-031-15777-6_22 (CCF-C, **Best Artifact Award**)
- **Wang Z.**, Zhang J., Liu Q., et al. Practical Metrics for Evaluating Anonymous Networks[C]. In 1st International Conference on Science of Cyber Security. Springer, Cham, 2018: 3-18. DOI: 10.1007/978-3-030-03026-1_1 (EI)
- Chen Y., Feng Y., **Wang Z.**, et al. IMaler: An Adversarial Attack Framework to Obfuscate Malware Structure against DGCNN-based Classifier via Reinforcement Learning[C]. In 2023 IEEE International Conference on Communications (ICC). IEEE, 2023. (CCF-C)
- Wang X., Liu C., Hu X., **Wang Z.**, et al. Make Data Reliable: An Explanation-powered Cleaning on Malware Dataset Against Backdoor Poisoning Attacks[C]. In Annual Computer Security Applications Conference (ACSAC), ACM, 2022: 267–278. DOI: 10.1145/3564625.3564661 (CCF-B)
- Zhang F., Cui X., **Wang Z.**, et al. A Systematic Study of AI Applications in Cybersecurity Competitions[C]. In 2020 IEEE 14th International Conference on Big Data Science and Engineering (BigDataSE). IEEE, 2020: 138-146. DOI: 10.1109/bigdatase50710.2020.00026 (EI)
- Yin J., Cui X., Liu C., Liu Q., Cui T., and **Wang Z.**. CoinBot: A covert botnet in the cryptocurrency network[C]. In 22nd International Conference on Information and Communications Security (ICICS). Springer, Cham, 2020: 107-125. DOI: 10.1007/978-3-030-61078-4_7 (CCF-C)
- Zhao Z., Liu Q., Song T., **Wang Z.**, and Wu X. WSLD: detecting unknown webshell using fuzzy matching and deep learning[C]. In 21st International Conference on Information and Communications Security (ICICS). Springer, Cham, 2019: 725-745. DOI: 10.1007/978-3-030-41579-2_42 (CCF-C)
- Liu C., Cui X., **Wang Z.**, et al. MaliceScript: A Novel Browser-Based Intranet Threat[C]. In 2018 IEEE 3rd International Conference on Data Science in Cyberspace. IEEE, 2018: 219-226. (EI)
- Liu J., Zhao Z., Cui X., **Wang Z.**, et al. A Novel Approach for Detecting Browser-Based Silent Miner[C]. In 2018 IEEE 3rd International Conference on Data Science in Cyberspace. IEEE, 2018: 490-497. (EI)
- Zhang J., **Wang Z.**. Poster: An anonymity metric of anonymous network[C]. In 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018. (CCF-A Poster)
- Su J., Liu Q., **Wang Z.**, Li X.. Poster: A Web Server Identified Model based on Mean Shift[C]. In 2018 IEEE Symposium on Security and Privacy (SP). IEEE, 2018. (CCF-A Poster)

专利

- 一种符合数据安全的威胁情报共享方法及装置, 第四申请人, 已公布, CN114553403A
- 一种基于参数水印的神经网络模型版权保护方法及装置, 第二申请人, 已申请

奖项证书

学科竞赛类

国际信息与通信安全会议（ICICS 2022） *Best Artifact Award* 2022 年 9 月
DataCon 大数据安全分析比赛网络流量分析 一等奖 2021 年 10 月
Coremail 邮件安全分析比赛 优胜奖 2020 年 10 月
DataCon 大数据安全分析比赛僵尸网络分析 优胜奖 2020 年 10 月
全国大学生信息安全竞赛 一等奖 2015 年 8 月

荣誉称号类

中国科学院大学学业奖学金一等奖 2021 年 9 月
中国科学院信息工程研究所所长优秀奖 2021 年 5 月
中国科学院大学优秀学生干部、三好学生 2019 年 5 月
中国民航大学人民奖学金一等奖 2015 年 12 月
中国民航大学优秀共青团员 2014 年 5 月、2015 年 5 月、2016 年 5 月

外语水平

大学英语六级 (CET-6) 521 分
大学英语口语 (CET-SET) B 级
全国英语等级考试五级 (PETS-5) 合格

校园经历

- 中科院信工所内训师 负责所内党支部党课及党史培训讲解工作
- 中科院信工所六室学生会副主席 负责学生招生和答辩工作，协助完成研究室集体活动
- 中国民航大学易航工作室部长 负责易航网维护、相关技术培训

(更新时间：2023-01-19)