

高明哲

东南大学计算机网络和信息集成教育部重点实验室
gmz9976.github.io (主页)

151-5053-2663 (电话)
mzgao@njnet.edu.cn (邮件)
<https://mzgao.blog.csdn.net> (博客)

教育经历

- 东南大学** 硕士学位
网络空间安全学院 · 计算机技术 2019.09 – 2022.03
 - 导师: 龚俭, 杨望
 - 毕业论文: 《基于串行架构的恶意软件家族识别方法研究》
 - 江苏省网络空间安全学会优秀硕士学位论文
 - 计算机网络和信息集成教育部重点实验
- 山东理工大学** 学士学位
计算机科学与技术学院 · 软件工程 2015.09 – 2019.06
 - 导师: 王凤英, 赵金铃
 - 毕业论文: 《基于卷积神经网络的恶意代码家族标注》

工作经历

- 阿里云** 安全攻防
云安全中心/WAF 产品能力建设 2022.07 – 至今
 - 研究方向 1: 基于程序切片的 PHP 源代码识别, 用于降低 Webshell 检测引擎误报
 - 研究方向 2: 验证码行为轨迹分析处置/Anti-Bot 能力建设
- 腾讯 (远程实习)** 安全研究
科恩实验室 2022.01 – 2022.04
 - 研究方向: 面向 source-code 的开源代码复用分析
- 奇安信-清华大学联合研究中心 (实习)** 安全研究
星图实验室 2020.11 – 2022.01
 - 合作导师: 应凌云
 - 研究方向: 基于 Learning 的恶意样本检测、家族标注、概念漂移、对抗性构造等

论文

- 《Rectify the Malware Family Label via Hybrid Analysis》 *《Computer Security CCF-B》* 2022.09
- 《一种基于多特征集成学习的恶意代码静态检测框架》 *《计算机研究与发展 CCF-T1》* 2020.12

专利

- 《一种基于混合分析的恶意软件家族标签更正方法及系统》 专利号: CN202210444025.5 2022.08
- 《一种恶意代码家族分类检测方法》 专利号: CN201910924383.4 2020.01

硕士经历

- 2022.03-2022.06, 基于 ARM 架构的 IOT 嵌入式设备的自动化 ROP 利用方法研究
- 2022.01, 提前毕业, 硕士论文拟推荐优秀毕业论文
- 2021.09-2021.11, 负责编纂互联网基础设施与软件安全年度发展研究报告中关于 AV 标签测量等部分章节

- 2021.05-2021.05，于山东理工大学做学术报告《恶意软件识别方法研究》
- 2021.01-2021.01，为华为-安恒 AI 安全冬令营结营赛提供数据安全题目支撑
- 2020.07-2020.12，参与开发东南大学-华为公司北向生态建设 Mediator 项目
- 2020.01-2020.01，参加 xman 赛宁网安冬令营成都 pwn 营，获结业证书

获奖情况

- 强网杯人工智能挑战赛 一等奖 2021.11
- DataCon 大数据安全竞赛物联网自动漏洞挖掘方向 前十名 2021.11
- 纵横杯网络安全技术创新大赛 二等奖 2021.11
- CCF 基于人工智能的恶意软件家族分类赛题 第四名（参赛队长） 2021.09
- DataCon 大数据安全竞赛恶意代码方向 优胜奖（参赛队长） 2020.08
- 百度 AI 安全对抗赛 第八名，三等奖（参赛队长） 2020.01
- 天融信杯 2018 第三届全国高校密码数学挑战赛 华东赛区二等奖（参赛队长） 2018.08
- 2017 高校网络信息安全管理运维挑战赛 华东赛区三等奖 2017.11
- 第六届山东省网络安全技能大赛 学生团队二等奖，个人三等奖； 2017.11
- 第十五届山东省大学生软件设计大赛 团队三等奖 2017.10
- 山东省物联网创新应用大赛——网络空间安全攻防赛 团队万腾杯三等奖 2017.09
- 2017 山东理工大学校级大学生创新创业项目 校级结项证书 2017.07
- 一等奖学金 校级 2018.11
- 一等奖学金 校级 2017.11