ZANDER WORK

zander@zanderwork.com
www.linkedin.com/in/zanderwork

Education

M.A., SECURITY STUDIES | Georgetown University | Fall 2021 – Spring 2023

- Concentration: Technology and Security

B.S., COMPUTER SCIENCE (SECURITY) | Oregon State University | 3.87 GPA | Fall 2017 - Spring 2021

- Key Courses: Intro to Digital Forensics, Operating Systems I and II, Systems Security, Cyber Attacks & Defenses
- Leading a senior capstone project to design infrastructure for the Oregon Research & Teaching Security Operations Center (ORTSOC), a student-staffed Security Operations Center (SOC) designed to vocationally teach students how a SOC works and how to be a security analyst
- Member of Dr. Yeongjin Jang's research group (SSH Lab), focusing on system and software security vulnerabilities. Worked on research projects targeting Apple iPhone/iOS, Intel CPUs, and Docker/container technology

Skills

Security

- Malware Analysis (IDA Pro/Hex-Rays Decompiler, Ghidra, Binja, gdb, x64dbg)
- Binary Exploitation (pwntools, angr)
- Vulnerability Scanning (Nessus, OpenVAS)
- Network Security (Zeek, Wireshark, nmap)
- Log Analysis (Splunk, Elastic, Azure Sentinel)

Infrastructure

- Virtualization (VMware vSphere, VMware Workstation, VirtualBox)
- Cloud Computing (AWS, GCP, DO, Azure)
- Infrastructure as Code (Terraform, Ansible)
- Containerization (Docker, Kubernetes)
- Rapid Prototyping (Vagrant)

Programming

- C, C++
- Python, *sh, PowerShell
- HTML/CSS/JS/SQL
- Django/Flask
- x86 Assembly
- Git

Work Experience

SECURITY ANALYST | Oregon State University Security Operations Center | October 2017 – Current

- Work with Zeek, Nessus, Splunk, and Azure Sentinel to perform network monitoring & analysis (max 100Gbps traffic)
- Design, deploy, and support production and development infrastructure
- Help lead incident response efforts by analyzing logs and performing forensic analysis on compromised Windows and Linux systems
- Develop automation to improve analysis efficiency by over 50%
- Monitor and respond to end-user phishing incidents
- Contribute to documentation and training materials for other team members

TECHNICAL INTELLIGENCE ANALYST INTERN | FireEye, Inc. | June 2019 – May 2020

- Deploy and integrate a sandbox environment for automated Android malware analysis for use across the entire company
- Analyze and process intelligence on financial crime threat activity to write reports for customers
- Profile and manipulate attacker Command & Control servers to learn more about their malware communications
- Hunt for and analyze malware samples from internal and external sources to support intelligence analysis
- Contributed to internal tracking of threat actors, malware samples/families, and TTPs
- Research published on the FireEye Blog: https://www.fireeye.com/blog/threat-research/2020/01/saigon-mysterious-ursnif-fork.html

Activities/Awards

OSU Security Club (2017 - 2021)

- Club president from 2017-2020, 250+ members
- Captain for competition teams (OSUSEC)
- Lead organizer for DamCTF, a Capture the Flag competition with over 700 teams in 2020
- Work with industry partners to bring recruitment events and presentations to our club members

NW Cyber Camp (2016 - 2019)

- Co-founded in 2016
- 5 sessions with over 100 total participants
- Weekly management meetings
- Work with local high schools for recruitment
- Coordinate with industry partners to secure funding and guest speakers

Recent Awards

- 3rd place, DOE Cyberforce Competition 2020 (remote, individual)
- 2nd place, Pacific Rim Collegiate Cyber Defense Competition 2020 (remote, team)