Daniel Mayer

Los Angeles, CA | https://www.linkedin.com/in/daniel-w-mayer/ | daniel.william.mayer@gmail.com

Professional Experience

SpecterOps, Inc | Los Angeles, CA

Consultant **July 2023 – Present**

- Execute bespoke offensive security and application security assessments including binary reverse engineering, vulnerability identification, and attack path assessment via kubernetes and active directory abuse.
- Contribute to course development and deliver trainings on reverse engineering and adversary tradecraft as an instructor of Adversary Tactics: Tradecraft Analysis
  - Delivered at Black Hat 2024
  - Delivered at SO-CON 2024
  - Delivered at over 5 other public and private training events
- Perform capability development for the Adversary Simulation team, developing new tools in C++ and C# to aid in post-exploitation activities during red team assessments
- Researched and executed the transition of the Adversary Simulation team's CI/CD pipeline from Jenkins to GitHub Actions
- Reverse engineer games in my free time, creating PoC cheats exploiting game logic vulnerabilities and reporting vulnerabilities to the developers:
  - Magic: The Gathering instant win exploit
  - Magic: The Gathering integer overflow in purchasing logic

Stairwell, Inc | Santa Cruz, CA

Threat Researcher **August 2022 – July 2023**

- Sole researcher on Stairwell's Threat Research team
- Responsible for helping develop Stairwell's products to aid in the static analysis and detection of malware through enterprise-wide YARA scanning.
- Implemented a CAPE Sandbox service allowing for malware detonation results for files analyzed by the product
- Drove product design decisions and test-drove the product to conduct my research.
- Statically analyzed malware in IDA and produced research in the form of reports, malware configuration extractors and signatures to aid in the programmatic detection and classification of malware.
- Some of my work included open-source contributions to CAPE sandbox, a report on emerging data extortion tactics, and analysis of a family of previously unidentified C++ Linux malware.

CrowdStrike, Inc | Santa Cruz, CA

Senior Security Researcher - Technical Analysis Cell **September 2019 – August 2022**

- Statically analyzed malware in IDA for CrowdStrike Intelligence's customers, in addition to internal customers such as CrowdStrike's professional services division and other intelligence analysts.
- Wrote and maintained malware configuration extractors in Python, wrote finished intelligence and signatures for customers, and helped train newer members of our team and improved processes
- Released private finished intelligence, in addition to sanitized blogs on noteworthy Threat Actors:
  - Blog on reverse-engineered malware targeting telecommunication companies

CrowdStrike, Inc | Washington, DC

Consultant - Incident Response **August 2018 – September 2019**

- Led small teams to investigate and help remediate eCrime and nation-state-backed intrusions for CrowdStrike's professional services division.
- Gained proficiency in host-based (dead disk and memory) forensic analysis techniques and procedures using XWays and Volatility, as well as network traffic and log analysis techniques and procedures using WireShark and Splunk.
- Developed efficient techniques for analyzing large amounts of forensic data accumulated from enterprise-wide forensic triage collections in Splunk, in addition to using the CrowdStrike Falcon platform for detection and response.

EDUCATION

Recurse Center | New York, NY **July, 2018**

Self-Directed:

- Spent 3 months in a batch at the self-directed programming retreat known as the Recurse Center, mainly studying security concepts and pair-programming with my batchmates.

Carleton College | Northfield, MN **August 2018**

B.A. Computer Science:

- Graduated with distinction

SKILLSETS

Tools: : IDA Pro/Hexrays, x64dbg, DNSpy, Cobalt Strike, Impacket, Mythic, Splunk, XWays, Volatility, Wireshark, Burp Suite, Encase, Microsoft Office/GSuite, AWS, Azure, GCP, Kubectl, IceKube, Jenkins, GitHub Actions, Git

Languages: Python, C/C++, C#, JavaScript, x86 Assembly, YARA, Snort, Bash/zsh, PowerShell