Micah Flack

36360 County 39
Laporte, MN 56461
jobs@micahflack.com
(218) 252-9797

EDUCATION

Dakota State University, Madison SD — *M.S. Computer Science*

Graduated Fall 2020

GPA: 4.0

Dakota State University, Madison SD — *B.S. Cyber Operations*

Graduated Fall 2019

GPA: 3.60

EXPERIENCE

Idaho National Labs, Idaho Falls ID — *Cyber Security Intern*

May 2020 - Now

- Broad understanding of threat intelligence formats and conversion techniques (MISP/Mitre Attack/TAXII/STIX)
- Use of relational graphs for both supervised and unsupervised machine learning modeling of extracted features from raw samples and threat intel
- Use of reverse engineering tools (IDA/Binary Ninja/Angr) for analysis of malware and extracted firmware.
- Remote/Telecommute from home office

Northrop Grumman, Cincinnati OH — *Cyber Security Intern*

May 2019 - August 2019

- Vulnerability research
- Hardware hacking over serial debug ports (JTAG/UART) with Shikra
- Bootloader memory scraping and firmware disassembly with Ghidra/Radare2
- Held an interim top-secret clearance

1st Financial Bank USA, Sioux Falls SD — *Security Analyst*

February 2018 - May 2019

- Used collated information to identify, analyze, and report events that occur or might occur within the network to protect information, information systems, and networks from threats.
- Security Information and Event Management (SIEM)
- Incident Response/Policy Creation
- Remote/Telecommute from home office

Dakota State University, Madison SD — *Teacher's Assistant*

January 2018 - Spring 2019

- CSC-304 Assembly Language

Dakota State University, Madison SD — *Cyclops/Student Researcher*

August 2017 - December 2018

- Sandboxing/Creating complete VM environments (VMWare, VirtualBox, Docker)
- Dynamic/Static analysis of malicious binaries (IDA/Radare2/Ghidra)
- Recognizing executable file formats (PE, ELF)
- Detection of packers/obfuscators
- Identifying use of Windows API (DLLs/Libraries, Functions)
- YARA signature creation and scripting

AWARDS

SFS CyberCorps Scholarship - Dakota State University/NSF

CLUBS

Dakota State University, Madison SD

August 2020 - May 2021

- President of Malware Club

PERSONAL PROJECTS

TEMPEST

- Dissection of electromagnetic emissions produced when keys are pressed on keyboards (e.g. PS/2, USB, 2.4GHz WiFi) then captured with a digital software defined radio (SDR).

DNS Rebinding

- Using a malicious DNS server to serve false DNS responses and gain access to devices behind NATed/private networks.

Undergrad. Research: Bust-A-Binary

- Deployable, open web-platform for malware analysis complete with threat feeds and simplified breakdown of binaries or other content.

Grad. Research: Feature Extraction and Analysis of Binaries for Classification

- Used Python3 and Pefile to extract basic header/section information from preprocessed PE32 samples routinely gathered from VirusTotal and HybridAnalysis. Features extracted were built into datasets for use with supervised machine learning languages from Scikit-learn. Overall achieved ~96-100% macro accuracy when positively classifying malware samples.

Flare-On and Codebreaker Challenges

- Application of reverse engineering techniques to challenges to recover flags or expand progress towards completion - Static/Dynamic Analysis