

# Nicholas B. Anderson

SECURITY ENGINEER · HOST BASED SECURITY DETECTION AND RESPONSE · MALWARE REVERSE ENGINEERING

✉ nanderson7@gmail.com | 🏠 brewfault.io | 📺 muffins | 📺 nanderson7 | 🐦 @poppyseedplehrz

## Experience

### Google Senior Security Engineer, Malware Reverse Engineer

Seattle, WA Sept. 2022 - Current

- Reverse engineered Android Applications to aid in developing detection signal for blocking apps installed on millions of Android devices
- Performed Red Team assessments against Android malware detection pipelines for Play Apps
- Performed Red Team assessments of on-device SDKs used for antimalware and message integrity
- Audited Android applications using Accessibility features and worked with engineering teams to propose platform solutions to abuse
- Developed strategy for detection prioritization through Threat Vectors using MITRE ATTACK framework
- Developed new MITRE ATTACK techniques for mobile devices
- Team lead for group focused on detecting and preventing the use of Dynamic Code Loading on Google Play
- Developed and delivered curriculum for physical security to internal groups

### Meta Senior Security Engineer, Malware Reverse Engineer

Seattle, WA Nov. 2020 - Sept. 2022

- Leveraged Andro-guard to design new APK analysis capabilities for scaled malware detection
- Mentored junior analysts to develop their career
- In-depth analysis of the Facestealer family of APKs including development timeline to identified over 300 APKs actively stealing user accounts
- Re-architected internal Dynamic Analysis infrastructure used for identifying malicious applications at scale
- Developed automation libraries and toolkits for malware analysis workflows and report generation
- Collaborated with engineers to build authenticated intelligence CLI agent to improve engineer efficiency
- Reverse Engineering of Malware on (Windows, iOS, Android, macOS) to generate reports and signatures to prevent the spread of malware on Meta platforms
- Reverse Engineering of mobile SDKs (iOS and Android) to detect Ads fraud and abuse in third party applications
- Reverse Engineering mobile and native applications for vulnerability assessments to harden Meta owned enterprise endpoints and Oculus applications

### Apple Senior Product Security Engineer, Ecosystem Integrity Protection

Seattle, WA Mar. 2020 - Nov. 2020

- Lead and architected framework leveraging AWS and WWDR to prevent malicious applications from executing on macOS
- Unified analyst libraries and established engineering excellence on the team through deploying CI/CD and testing suites to code repository
- Reverse Engineered malware samples affecting macOS and published protective signatures deployed to endpoints

### Facebook Senior Security Engineer, Detection Infrastructure

Menlo Park, CA Feb. 2016 - Mar. 2020

- Core developer and maintainer of osquery project - <https://osquery.io>
- Lead security org to scale Endpoint Detection and Response infrastructure by migrating legacy on-prem infrastructure to cloud-hosted solution
- Lead enterprise endpoint security team to deploy Santa and AppLocker to corporate macOS and Windows endpoints
- Worked with security leadership to establish a new team focusing on enterprise endpoint security
- Purchase and integration of third-party Detection-as-a-Service capabilities
- Developed and maintained host-based endpoint monitoring agents, logging infrastructure, and deployment mechanisms
- Administered and orchestrated Carbon Black backend infrastructure and endpoint deployment
- Built endpoint detections leveraging host-based telemetry
- Mentored university students internationally for the Facebook Open Source Mentorship program
- Rearchitected corporate DNS deny-listing capability, increasing reliability and reducing operational overhead
- Developed and delivered security education curriculum for lockpicking and Capture The Flag challenges used in Hacktober security awareness month
- Developed and delivered osquery workshop curriculum for conferences to teach endpoint detection at scale

### Sandia National Laboratories Cyber Security R&D Scientist and Engineer

Albuquerque, NM Jan. 2015 - Jan. 2016

- Malware Reverse Engineer on Security Incident Response Teams
- Reverse Engineered and developed C2 generation script for detection of Hammertoss malware
- Mentored Albuquerque High School CyberPatriot team

### Sandia National Laboratories Graduate Student Intern, Center for Cyber Defenders (CCD)

Albuquerque, NM June 2014 - Aug. 2014

- Developed fuzzing framework for email detection engine to test corporate detection rules
- Researched automated vulnerability discovery methods for Windows binary files

### Trail of Bits Security Intern

New York, NY Jan. 2014 - Aug. 2014

- Developed platform testing framework for iterated Windows versions using Virtual Machine APIs

### Handel IT Software Developer, Systems Administrator

Laramie, WY Sept. 2012 - Aug. 2013

- C# and .NET software developer for RiteTrack5 software suite
- Systems Administrator for Windows 2003, 7, 2008, 2012, and FreeBSD(pfSense) Operating Systems
- Deployed and Administered Nagios Core to enterprise endpoints
- Administered Windows SCCM server for software deployments and endpoint compliances

### University of Wyoming, Mathematics Dept. Academic Lecturer

Laramie, WY Dec. 2009 - Apr. 2010

- Responsible for lectures, student grades, and preparing and issuing class quizzes

### University of Wyoming IT Technician for Academic Support Unit

Laramie, WY Feb. 2008 - July. 2009

- Troubleshooting computer issues, maintaining computer labs, and tech support

Education

<b>New York University, Polytechnic</b> <i>Master of Science in Cybersecurity, 3.889 GPA</i> <ul style="list-style-type: none"><li>SFS ASPIRE Fellowship</li></ul>	Brooklyn, NY
<b>University of Wyoming</b> <i>Master of Science in Mathematics, <b>Dropped Out</b>, 3.42 GPA</i> <ul style="list-style-type: none"><li>Computing the refined stability condition, Quarterly of Applied Mathematics</li><li>Upsilon Pi Epsilon Special Recognition Scholarship Recipient, Fall 2012</li></ul>	Laramie, WY
<b>University of Wyoming</b> <i>Bachelor of Science in Mathematics, Minor in Computer Science, 3.883 GPA</i> <ul style="list-style-type: none"><li>Outstanding Graduate, College of Arts &amp; Sciences Top 20 in Class, Spring 2010</li><li>Honor Roll, U.W. President's List, 4.0 Semester GPA, Spring 2007, 08, 09</li><li>Varineau Memorial Math Scholarship Recipient, Spring 2009</li></ul>	Laramie, WY

## Conference Talks & Workshops

Oct. 2018	<b>OSDFcon</b> , The osquery file carver	Herndon, VA, USA
Oct. 2018	<b>OSDFcon</b> , Docker Detection and Forensics, 'Gotta catch them all'!	Herndon, VA, USA
June 2018	<b>QueryCon</b> , Keynote - Evolving Our Open Source Community	San Francisco, CA, USA
Nov. 2018	<b>BlueHat</b> , Detecting compromise on Windows endpoints with osquery	Redmond, WA, USA
Oct. 2016	<b>Brucon 0x8</b> , Hunting Malware at Scale with osquery	Ghent, Belgium
Sept. 2016	<b>Structure Security</b> , Open Source Security Panel	San Francisco, CA, USA
Aug. 2016	<b>DEFCON 24</b> , Hunting Malware at Scale with osquery	Las Vegas, NV, USA
Aug. 2015	<b>DEFCON 23</b> , Hardware and Trust Security: Explain it like I'm 5	Las Vegas, NV, USA

## Publications

### Introducing osquery for Windows

<https://www.facebook.com/notes/protect-the-graph/introducing-osquery-for-windows/1775110322729111/>

*Protect the Graph* Sept. 27th, 2016

### Computing the refined stability condition <https://arxiv.org/abs/1207.4101>

*University of Wyoming* July 17th, 2012

## Skills

<b>Programming</b>	Python, C, C++, Intel x86/x64 and ARM Assembly, Powershell, Hacklang, sqlite, R
<b>Security Tools</b>	IDA Pro, BinaryNinja, WinDBG, gdb, Wireshark, nmap, x64dbg, ollydbg, Metasploit, Empyre
<b>Enterprise Tools</b>	osquery, Chef, Splunk, Graylog, AWS (EC2, Lambda, SQS SNS, ECS, CloudFormation), MD-ATP, Windows Active Directory, pfSense, Carbon Black
<b>Fields of Interest</b>	Malware Reverse Engineering, Digital Forensics, Cloud Infrastructure for Detection and Response, Exploitation, Lockpicking, CTFs

## Honors & Awards

2017, 2019	<b>Splunk Boss of the SoC</b> , Regional Winners	Seattle, WA, US
2017	<b>O'Reilly Security Conference</b> , O'Reilly Security Project Defender Award	New York, NY, US
2014, 15, 17	<b>FireEye flare-on Reverse Engineering CTF</b> , Completed and Honor Roll	<a href="http://flare-on.com">flare-on.com</a>

## Associations

2009 - 2010	<b>Researcher</b> , Cryptography Research Cohort	University of Wyoming
2009	<b>Researcher</b> , NSF EPSCoR Research Fellowship	University of Wyoming
2009 - 2012	<b>Founding Charter Member</b> , Upsilon Pi Epsilon	University of Wyoming
2009 - 2012	<b>Founding Member and Co-Captain</b> , Cyber Defense Action League, University of Wyoming Cybersecurity Team	University of Wyoming

## Extracurricular Activity

### Brooklynt Overflow, NYU OSIRIS Lab *Co-Captain and Team Lead*

*Brooklyn, NY* 2013 - 2015

- Curator of educational program Hack Night, teaching new students about security
- Organizer of CSAW Security Conference
- CTF Challenge author for DHS Forensics competition

### Cyber Defense Action League, Univ of Wyo Cyber Security team *Core and Founding Member*

*Laramie, WY* 2009 - 2012

- Helped found and establish the University of Wyoming Cybersecurity team
- Awarded \$15,271.26 for grant proposal to construct Cyber Security Lab
- 1st Place Winner of the North Central Collegiate Cyber Defense Competition in Spring 2011, 12
- Competed in CTF competitions such as CSAW, ASIS, Plaid, and ruCTF
- Gave educational demos around exploitation and malware reverse engineering

### Upsilon Pi Epsilon *Founding Charter Member*

*Laramie, WY* 2009 - 2012

- Helped found and establish the University of Upsilon Pi Epsilon (Computer Science Honor Society) chapter

### University of Wyoming Cryptography Research Cohort *Researcher*

*Laramie, WY* Academic year 2009 - 2010

- Worked with cohort on deep dives into asymmetric crypto routines and co-prime primitives
- Wrote R code for running numerical analysis of research work

### NSF EPSCoR Research Fellowship *Researcher*

*Laramie, WY* Spring 2009

- Senior research project the analysis of eigenvalues of different wave forms