Nicholas B. **Anderson**

Security Engineer · Host Based Security Detection and Response · Malware Reverse Engineering

nanderson7@gmail.com | brewfault.com | muffins | nanderson7

Experience

Google *Senior Security Engineer, Malware Reverse Engineer* — *Seattle, WA Sept. 2022 - Current*

- Reverse Engineered Android applications and developed detections to block the install of apps on millions of devices globally
- Developed automation tooling to assist in reversing applications making use of popular frameworks (Flutter/Unity)
- Developed framework for automated firmware scraping of Android TV devices for identifying preloaded backdoors
- Identified techniques used by malware to evade detections accounting for over 1M+ installs in off-Play Android devices
- Lead multiple working groups to address various detection gaps in Play detection pipelines including Dynamic Code Loading, architecting capabilities to surface new Android malware via C2 communications, and most recently efforts to formalize our threat hunting capabilities
- Directly mentored junior engineers, interns, and Nooglers on career advancement as part of internal mentorship programs
- Reverse Engineered internal SDKs used for anti-malware and message integrity as part of Red Team assessments
- Reverse Engineered Play store applications making use of Accessibility services in a store wide audit of Accessibility abuse
- Developed framework for detection prioritization through Threat Vectors using MITRE ATTACK framework
- Authored multiple new MITRE ATTACK techniques unique to attacks on mobile devices
- Developed and delivered curriculum for reverse engineering techniques of framework applications (flutter/unity), as well as physical security to internal teams and groups

Meta *Senior Security Engineer, Malware Reverse Engineer* — *Seattle, WA Nov. 2020 - Sept. 2022*

- Re-architected internal Dynamic Analysis infrastructure used for identifying malicious applications at scale
- In-depth analysis of the Facestealer family of APKs including development timeline to identified over 300 APKs actively stealing user accounts
- 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
- Developed automation libraries, toolkits for analysis workflows, and an authenticated CLI agent to increase engineering efficiency
- Reverse Engineering mobile and native applications for vulnerability assessments to harden Meta owned enterprise endpoints and Oculus applications
- Directly mentored junior analysts and engineers to accelerate career development

Apple *Senior Product Security Engineer, Ecosystem Integrity Protection* — *Seattle, WA Mar. 2020 - Nov. 2020*

- Architected a framework leveraging AWS and WWDR to prevent unauthorized application execution 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*

- Served as a core maintainer and developer for the osquery project, scaling endpoint monitoring agents and logging infrastructure
- Led the migration of legacy endpoint detection back-end infrastructure to cloud-hosted solutions
- Worked with leadership to establish new team focused on enterprise security capabilities
- Deployed and maintained multiple security endpoint agents to corporate and production fleets, such as Santa, AppLocker, and Carbon Black
- Rearchitected corporate DNS deny-listing for increased reliability
- Authored endpoint detections for malware campaigns and worked with Incident Response teams to develop runbooks and automations for forensics
- Developed and delivered global curricula for lockpicking, CTFs, and osquery workshops for conferences and internal awareness
- Mentored numerous engineers in the osquery ecosystem including students through Facebooks Open Source mentorship program

Sandia National Laboratories *Cyber Security R&D Scientist and Engineer* — *Albuquerque, NM Jan. 2015 - Jan. 2016*

- Reverse engineered multiple malware families and campaigns, such as the Hammertoss malware and developed detection signatures (Yara) as well as DGA scripts for C2 tracking
- Researched automated vulnerability discovery techniques for Windows binaries
- Mentored Albuquerque High School CyberPatriot team

Handel IT *Software Developer, Systems Administrator* — *Laramie, WY Sept. 2012 - Aug. 2013*

- Administered Windows and FreeBSD (pfSense) systems while deploying Nagios and SCCM for endpoint compliance
- Developed C# and .NET applications for the RiteTracks software suite

Education

New York University, Polytechnic *Master of Science in Cybersecurity, 3.889 GPA* — *Brooklyn, NY*

- SFS ASPIRE Fellowship

University of Wyoming *Master of Science in Mathematics, **Dropped Out**, 3.42 GPA* — *Laramie, WY*

- Computing the refined stability condition, Quarterly of Applied Mathematics
- Upsilon Pi Epsilon Special Recognition Scholarship Recipient, Fall 2012

University of Wyoming *Bachelor of Science in Mathematics, Minor in Computer Science, 3.883 GPA* — *Laramie, WY*

- Outstanding Graduate, College of Arts & Sciences Top 20 in Class, Spring 2010
- Honor Roll, U.W. President's List, 4.0 Semester GPA, Spring 2007, 08, 09

Conference Talks & Workshops

Oct. 2025	**AMTSO 2025,** Joker hates this one weird trick! - Taking down Joker Toll Fraud campaigns using server misconfigurations	*Lisbon, Portugal*
Aug. 2024	**0x0G,** Emerging Malware Threats in the Off-Market Space	*Las Vegas, Nevada, USA*
Oct. 2018	**OSDFcon,** The osquery file carver	*Herndon, VA, USA*
Oct. 2018	**OSDFcon,** Docker Detection and Forensics, 'Gotta catch them all'!	*Herndon, VA, USA*
June 2018	**QueryCon,** Keynote - Evolving Our Open Source Community	*San Francisco, CA, USA*
Nov. 2018	**BlueHat,** Detecting compromise on Windows endpoints with osquery	*Redmond, WA, USA*
Oct. 2016	**Brucon 0x8,** Hunting Malware at Scale with osquery	*Ghent, Belgium*
Sept. 2016	**Structure Security,** Open Source Security Panel	*San Francisco, CA, USA*
Aug. 2016	**DEFCON 24,** Hunting Malware at Scale with osquery	*Las Vegas, NV, USA*
Aug. 2015	**DEFCON 23,** 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

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

Honors & Awards

2017, 2019	**Splunk Boss of the SoC,** Regional Winners	*Seattle, WA, US*
2017	**O'Reilly Security Conference,** O'Reilly Security Project Defender Award	*New York, NY, US*
2014, 15, 17	**FireEye flare-on Reverse Engineering CTF,** Completed and Honor Roll	*flare-on.com*
2009	**NSF EPSCOR,** Research Fellowship	*University of Wyoming*