BILL DEMIRKAPI

https://billdemirkapi.me

Education

BS, Computing Security — 2019 to 2023
Rochester Institute of Technology

Experience

Security Engineer II — May 2022 to Present
Microsoft

- Lead vulnerability response to multiple in-the-wild zero-days in Microsoft products.
- Developed multiple mitigation strategies to eliminate frequently abused attack surface.
- Awarded "Outstanding Contribution" MSRC Polaris award within two months of joining.

Senior Security Engineer — November 2021 to March 2022
Zoom

- Performed multiple objective-oriented black box assessments of corporate infrastructure.

Application Security Engineer — August 2020 to November 2021
Zoom

- Audited the applications our company uses for security vulnerabilities.
- Created an automated microservice platform on AWS that actively remediates a common vulnerability class. Platform found & remediated $700,000+ worth of vulnerabilities.

Security Intern — April 2020 to August 2020
Zoom

- Hired by the CEO of Zoom at the peak of the pandemic to help the Engineering Security team.

Software Engineering Intern — June 2019 to August 2019
CrowdStrike

- Developed anti-tamper solutions for core parts of the CrowdStrike Falcon sensor under the Strategic Research Initiatives team.

Security Integration Engineer High School Intern — June 2018 to August 2018
IBM Resilient

- Integrated security products with the Resilient incident response platform.

Conference Talks

DEF CON 32 – Secrets and Shadows: Leveraging Big Data for Vulnerability Discovery at Scale	August 2024
Black Hat USA – Locked Down but Not Out: Fighting the Hidden War in Your Bootloader	August 2024
Black Hat USA – Predict, Prioritize, Patch: How Microsoft Harnesses LLMs for Security Response	August 2024
Offensive Con – Booting With Caution: Dissecting Secure Boot's Third-Party Attack Surface	May 2024
Black Hat USA *and* DEF CON 31 – A SSLippery Slope: Unraveling the Dangers of Certificate Misuse	August 2023
SecTor 2020 – Demystifying Modern Windows Rootkits	October 2020
Black Hat USA *and* DEF CON 28 – Demystifying Modern Windows Rootkits	August 2020
DEF CON 27 – Are Your Child's Records at Risk? The Current State of School Infosec	August 2019
RECon Montreal 2019 – The Unseen Dangers of Bloatware	June 2019

Research Publications

Abusing Exceptions for Code Execution, Part 2	bit.ly/45QeZRn
Unpacking CVE-2021-40444: A Deep Technical Analysis of an Office RCE Exploit	bit.ly/3NI0urD
Process Forking: Abusing Windows' Implementation of Fork() for Stealthy Memory Operations	bit.ly/314Xsdq
Insecure by Design, Epic Games Peer-to-Peer Multiplayer Service	bit.ly/34NKq2K
How to use Trend Micro's Rootkit Remover to Install a Rootkit	bit.ly/3caDZ
Hacking College Admissions	bit.ly/2Kh3GO8
Remote Code Execution in all Dell machines via pre-installed software	bit.ly/2PGTluf