BILL DEMIRKAPI
billdemirkapi@gmail.com
https://billdemirkapi.me

Education

BS, Computing Security — Expected May 2023
Rochester Institute of Technology

Experience

Application Security Engineer — August 2020 to Present
Zoom Video Communications

- Leading the engineering of red team tooling for assessments as the technical architect and primary contributor.
- Auditing the applications our company uses for security vulnerabilities.

Security Intern — April 2020 to August 2020
Zoom Video Communications

- As a Security Intern, my role focuses on securing the Zoom client by engineering solutions to prevent future vulnerabilities and managing the development of vulnerability patches.

Windows Red Team Engineer — January 2020 to Present
RITSEC Red Team

- Designed custom malware used in popular blue team competitions such as RIT's IRSec and Lockdown at the University of Buffalo.

Windows Penetration Testing Lead — September 2019 to November 2019
RIT Collegiate Penetration Testing Competition

- Led offensive Windows penetration testing operations as part of RIT's team for the Collegiate Penetration Testing Competition.

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 28 – Demystifying Modern Windows Rootkits — August 2020
Black Hat USA 2020 – 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

Defeating Macro Document Static Analysis with Pictures of My Cat — bit.ly/35ETXKR
How to use Trend Micro's Rootkit Remover to Install a Rootkit — bit.ly/3caDZ
Several Critical Vulnerabilities on most HP machines running Windows — bit.ly/2RyNZ6j
Insecure by Design: Weaponizing Windows against User-Mode Anti-Cheats — bit.ly/2rIRNbj
Remote Code Execution in Lenovo Service Bridge
Local Privilege Escalation in all Dell machines via pre-installed software — bit.ly/2kR0fBS
Improper Access Control in Admissions Software allowing students to accept themselves — bit.ly/2Kh3GO8
Arbitrary physical memory access in Carbon Black endpoint software — bit.ly/2lYKjOs
Remote Code Execution in all Dell machines via pre-installed software — bit.ly/2PGTluf