Charles K. Varga, Jr.

Eagle Scout • Aspiring Cybersecurity Researcher

Email : charles_varga_jr@icloud.com
Mobile : 301.300.5708

Education

- **Pace University** New York, NY
  Master of Science in Computer Science, 3.7 GPA *Jan. 2022 – May 2024 (expected)*
- **University of Maryland, Baltimore County** Baltimore, MD
  Bachelor of Science in Computer Science, 3.55 GPA *Aug. 2018 – Jan. 2021*
- **Montgomery College** Rockville, MD
  Associate of Arts in Computer Science, 3.31 GPA *Aug. 2016 – May 2018*

Experience

- **Florida Department of Financial Services** Tallahassee, FL
  Systems Programmer II *Apr. 2022 - Present*
  - Ensure network security and continuous availability of distributed services across a department which interacts with multimillion dollar financial institutions across the state of Florida.
  - Enterprise administrator of endpoint security and policy compliance solution which manages thousands of devices across the department network.
  - Subject matter expert of Splunk SIEM solution which ingests millions of network events on a daily basis.
- **Griffiss Institute, Inc./Assured Information Security, Inc.** Rome, NY
  Advanced Course in Engineering (ACE) Graduate Assistant *Nov. 2020 - Aug. 2021*
  - Mentored and supported future leaders of consequence through their progression in the ACE program.
  - Engaged in continuous leadership development through independent study and guided mentorship from government and military leaders.
  - Administrative leader of one of three teams in fictional cyber warfare exercise based on real global events.
  - Collected and analyzed intelligence and software in search of vulnerabilities as part of cyber and kinetic operations in simulated warfare.
  - Document deployment and exploitation of cloud-based virtual servers for purposes of red team exercises.
- **University of Maryland, Baltimore County** Baltimore, MD
  Graduate Research Assistant/Undergraduate Teaching Fellow *Sep. 2020 - Aug. 2021*
  - Researched malware analysis techniques as it pertains to the generalization of malware datasets to unforeseen malware specimens across multiple families.
  - Collaborated with a team of 10 to teach and prepare instruction material for an active cyber defense class.
  - Taught students how to secure common services on Linux machines.
  - Provided instruction on common web vulnerability exploitation techniques such as SQL injection and cross-site scripting.
- **Cyber Pack Ventures, Inc.** Baltimore, MD
  Research Assistant *Jan. 2020 - May 2021*
  - Conduct research on malware analysis in the large.
  - Adopt a data science-driven approach to discovering malicious code.
  - Worked with a team of 3 to write a Ghidra plugin that automates static analysis of raw binaries.
  - Trained a machine learning model to identify and distinguish malicious and benign functions within malware from extracted features.
- **Assured Information Security, Inc.** Rome, NY
  ACE Intern *Jun. 2020 - Aug. 2020*
  - Engaged in intensive cybersecurity bootcamp through rigorous coursework, research, leadership development, and field operations.
  - Participated in team and technical leadership development under mentorship from distinguished leaders in government and military.
  - Solved graduate level challenge problems in malware analysis, code-level attacks, hardware security, etc. after theoretical and hands-on instruction from subject matter experts.

  - Developed a red team targeting and analysis tool utilizing a Python/Django/Postgres/Docker technology stack in accordance with unit testing and continuous integration practices.
  - Created Golang based tooling and executed cyber operational objectives in support of team in large scale, multidomain, and long term training exercise.

- **Montgomery County Government** Rockville, MD
  Junior Security Engineer/Information Security Intern *Jan. 2018 - Dec. 2019*
  - Worked alongside industry-recognized security experts to practice cybersecurity. Performed incident response (IR) and penetration testing on the county's production network, which is funded by a $5 billion annual budget.
  - Converted technical results of penetration testing processes to risk and business impact analyses. Researched exploits for certain web servers to enhance team collaboration.
  - Utilized the County's central threat console, SIEM, asset and vulnerability management (VM) system, and help desk system to implement the IR procedure. Automated administrative tasks for IR.
  - Converted business and technical IR and VM processes to a realtime Security Operations Center display.
  - Prepared documentation for updated IR plan, based on the NIST SP-800 series.
  - Administered a Mongo database for monitoring of production network traffic.
  - Utilized open source intelligence (OSINT), packet sniffing software (Wireshark), and three different sandbox environments for malware analysis.
  - Configured an Ubuntu server for collecting internal asset information and OSINT on malicious communicating hosts.
  - Wrote Python scripts connecting to APIs to streamline and modernize the security team's IR procedure.

Publications

- E. Golaszewski et al., including **C.K. Varga**, "Project-based learning continues to inspire cybersecurity students: The 2018–2019 SFS research studies at UMBC," ACM Inroads, vol. 11, no. 2, pp. 46–54, 2020. https://doi.org/10.1145/3386363
- Boutsikas, J., Eren, M.E., **Varga, C.**, Raff, E., Matuszek, M., and Nicholas, C.. Evading Malware Classifiers via Monte Carlo Mutant Feature Discovery. Poster to appear in MTEM '21: Malware Technical Exchange Meeting, July 13-15, 2021, Sandia National Laboratories, Virtual Event, USA. https://arxiv.org/abs/2106.07860

Other Activities

- **US Cyber Combine / Accelerated Training Program** US Cyber Games
  Red vs. Blue Cyber Athlete *Jun. 2021 – Present*
  - Inductee into selective program which involves 6-month rotational training in web application security, reverse engineering, binary exploitation, etc. in teams of 4-5 athletes.
  - Participated in 10-week invitational program to practice cybersecurity skills in a competitive team-based environment of multiple styles such as Capture the Flag and Red versus Blue.
- **Scholarship For Service Research Study** UMBC
  Student Participant *Jan. 2020 – Jan. 2020*
  - Conducted a one-week security consultancy for the university's information technology team, which provides service to over 17,000 clients.
  - Collaborated with a team of 30 to conduct penetration tests on an internal university web application.

Certifications

- **CompTIA Security+** *Aug. 2019, Expires Aug. 2025*

Skills

- **Reconnaissance** : NMAP
- **Incident Response** : iBoss • Qualys • Zendesk • Trusted Metrics
- **Penetration Testing** : Wireshark • Burp Suite • OWASP ZAP • OWASP Dirbuster • Cobalt Strike
- **Software Development** : Pylint • Autopep8 • Flake8 • GCC/G++ • Valgrind
- **Reverse Engineering** : GDB • EDB • Ghidra • IDA • Immunity Debugger

- **Malware Analysis** : Regshot • YARA • FLARE VM • Detect It Easy • PEiD • Procmon • Autoruns • Strings • FLOSS
- **Operating Systems** : Ubuntu • Arch Linux • Kali • Parrot Security • Tails
- **Databases** : MongoDB
- **Web Frameworks** : Django • Hugo
- **Programming Languages** : Python • C/C++ • Shell • Bash • Go
- **Foreign Languages** : Portuguese (fluent) • Spanish (intermediate) • Hungarian (basic)

Recognitions

Montgomery Scholars Scholarship • Beacon Conference Finalist • Dean's List • President's List