Apurv Singh Gautam

apurvsinghgautam@gmail.com apurvsinghgautam.me

Professional Summary

I am a Cybersecurity researcher with 5 years of progressive experience seeking a Threat Intelligence Analyst role. I have experience with threat hunting on the surface web and dark web and analyzing and producing threat intelligence. I enjoy reading threat reports, white papers, and blogs. I have been attending and speaking at many conferences, including SANS, DEFCON RTV, Diana Initiative, and many more. I love being involved and contributing to the security community

Experience

- **IZon Group LLC** Atlanta, US
  Security Intern Sept 2020 - Present
  - **Area**: Threat Intelligence - Obtaining intelligence from dark web
  - Creating multiple crawlers/scrapers for collecting large scale data from the dark web forums
  - Analyzing data in the form of TTPs and storing it in Elasticsearch
  - Visualizing data in Kibana in the form of threat intel feeds
  - Mentoring an intern for public speaking in cybersecurity
- **Georgia Institute of Technology** Atlanta, US
  Head Teaching Assistant Aug 2019 - Present
  - **Course**: CS 4235/6035 Intro to Information Security, CS 6250-O01 Computer Networks
  - Managing 4 TAs and 160 students
  - Creating weekly quiz questions for different security topics
  - Grading assignments, quizzes, projects and exams
- **International Computer Science Institute, UC Berkeley** Berkeley, US
  Security Research Intern May 2020 - Jul 2020
  - **Area**: Threat Intelligence - Creating threat intelligence metrics
  - Performed deep dive analysis of malicious data from 4-5 dark web forums/markets
  - Analyzed the large unstructured data using advanced NLP algorithms (LDA, CatE)
  - Created 6 high-level threat intelligence metrics for the analyzed data
- **Volon Cyber Security Pvt. Ltd.** Pune, India
  Security Research Intern May 2018 - May 2019
  - **Area**: Threat Intel/Hunting - Obtaining Intelligence from surface/dark web forums
  - Performed advanced open source intelligence (OSINT) on surface web and dark web sites
  - Performed threat landscape analysis on dark web forums and markets
  - Created an advanced automated scraping tool to scrape data using Python Scrapy
  - Scraped unstructured data of about 10-20 dark web forums and markets into elasticsearch
  - Performed human intelligence (HUMINT) on the dark web forums and marketplaces
  - Conducting various threat investigations and preparing a finished report in the form of tactics, techniques, and procedures (TTPs)

Education

- **Georgia Institute of Technology** Atlanta, US
  Master of Science in Cybersecurity (M.S.); GPA: 3.75 2019 - Expected May 2021
  - **Relevant Coursework**: Network Security, Measurement & Security, Secure Computing Systems, Info Sec Policies, Binary Analysis Lab, Intro to Malware Reverse Engineering
- **Symbiosis Institute of Technology** Pune, India
  Bachelor of Technology in Information Technology (B.TECH); CGPA: 8.63 2015 - 2019
  - **Relevant Coursework**: Operating Systems, Computer Networks, Data Structures, Cloud Computing, Distributed Computing, Cybersecurity

Security Community Involvement

- **SANS OSINT Summit '21**: CFP Accepted for OSINT Tools for Diving Deep into the Dark Web
- **SANS Cyber Defense Forum '20, BSides Toronto '20, BSides Philly '20, BSides DFW '20, GrayHat Blue Team Village '20, RootCon '20, BSides Singapore '20, The Diana Initiative '20, DEFCON 28 Red Team Vilage '20**: Delivered a talk on Automating Threat Hunting on the Dark Web and other nitty-gritty things [Video]
- **GRIMMCon 0x2 '20**: Delivered a talk on Threat Hunting on the Dark Web [Video]
- **CTI League**: Volunteering as a Darknet researcher, creating crawlers and scrapers to scrape from the darknet for monitoring healthcare threats
- **Cybrary**: Volunteering as a Writer, previously as a Senior Teaching Assistant, managing security-fundamentals channel, creating materials for several security courses, including Intro to Threat Intelligence, Insider Threats, Intro to TOR, and many more
- **StationX**: Volunteering as a Teaching Assistant, moderating the discourse, engaging with the community, and solving course-related doubts

Skills

- **Programming**: Proficient in Python and Bash, Knowledge of C, C++, Java
- **Security**: Threat Intelligence, Threat Hunting, OSINT, HUMINT, Security Analysis, Incident Handling, Malware Analysis, Log Analysis
- **Tools**: Splunk, Yara, Syslog, Suricata, GDB, Ghidra
- **Miscellaneous**: Elastic Stack, MITRE ATT&CK, NLP, SIEM

Open Source Contributions

- **OnionIngestor**: OnionIngestor is based on ThreatIngestor tool structure to enable modular and extendable access for Cyber Threat Intelligence teams so that they can monitor and collect information on hidden sites over tor network. [GitHub]
  - Created 5 sources to extract .onion domains with 8 sources in total
  - Utilizes 4 operators including HTML source, screenshot, onionscan, and yara
  - Stores analyzed data into Elastic stack
  - Produces daily reports and sends the notification to Kibana and Telegram

Relevant Projects/Research Work

- **PastebinScrapy**: Threat Hunting tool built on Flask that scrapes IOCs, including IP addresses, hashes, and emails from Pastebin's latest pastes [GitHub]
  - Created an automated scraping tool using Python
  - Scrapes latest pastes from Pastebin using Pastebin's Scraping API
  - Collects IOCs like IP addresses, hashes, emails from the latest pastes using regex
  - Utilizes Elastic Stack to store the data and visualize it
  - Created dashboard using Flask to view and interact with data with search capabilities
- **Applying Diamond Model on WannaCry Ransomware Incident**: This blog maps WannaCry ransomware incident to the Diamond model that includes all components of the model [Blog Post]
  - Performed case analysis with diamond model including victim, infrastructure, capability, adversary
  - Discussed extended diamond model that includes social-political and technological meta feature
  - Performed case analysis with policy impact

Certifications/Trainings

- **SOC Analyst 1 Battle Path by Rangeforce**: (Ongoing)
- **Blue Team Level 1 by Security Blue Team**: (Ongoing)
- **Blue Team Junior Analyst by Security Blue Team**: (Dec 2020) [Link]
- **SOC Core Skills (16-hour) by John Strand**: (Nov 2020) [Link]
- **Vishy Little Liars - Pretexts That Kill workshop by Alethe Denis**: (Nov 2020) [Link]
- **Getting Started in Security with BHIS and MITRE ATTCK (16-hour) by John Strand**: (Jul 2020) [Link]
- **CompTIA Security+ ce by CompTIA**: (Feb 2019 - Feb 2022) [Link]