

Apurv Singh Gautam

apurvsinghgautam@gmail.com

apurvsinghgautam.me

PROFESSIONAL SUMMARY

I am a Cybersecurity researcher with 3 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, Diana Initiative, BSides, and many more. I love being involved and contributing to the security community

EXPERIENCE

- **Cyble Inc.** Atlanta, US
Threat Researcher Jul 2021 - Present
 - Conducting surface, deep, and dark web investigations, profiling threat actors & hacker groups, and researching ransomware attacks
 - Leading the US-based client requests by performing continuous monitoring and alerting regarding emerging threats within the surface and underground forums/markets
 - Producing concise finished intelligence reports for new findings within the surface, deep, and dark web related to our global clients
 - Responding to ad-hoc requests by US-based clients and producing detailed intelligence reports in the form of tactics, techniques, and procedures (TTPs)
 - Utilizing OSINT, SOCMINT, and HUMINT in leveraging new threat information from the surface, deep, and dark web
 - Designing and developing small-scale Python scripts to assist with automation of collection, processing, and storage of data and reducing the time load by 40%
- **IZon Group LLC** Atlanta, US
Security Intern Sep 2020 - Mar 2021
 - Created multiple crawlers/scrapers for collecting large scale data from the surface/dark web forums
 - Analyzed data in the form of TTPs and storing it in Elasticsearch
 - Visualized data in Kibana in the form of threat intel feeds and creating dashboards
- **International Computer Science Institute, UC Berkeley** Berkeley, US
Security Research Intern May 2020 - Jul 2020
 - 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 Researcher May 2018 - May 2019
 - 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

EDUCATION

- **Georgia Institute of Technology** Atlanta, US
Master of Science in Cybersecurity (M.S.); GPA: 3.78 2019 - 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 New to Cyber Summit '21:** Delivered a panel talk with 3 other speakers on Hack Your Growth - #LevelUP
- **SANS OSINT Summit '21:** Delivered a talk on 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 Village '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 [\[Video\]](#)
- **Evidence-Based Cybersecurity Group (EBCS):** Volunteering as a Darknet researcher, creating crawlers and scrapers to scrape from the darknet for monitoring threats related to several sectors like healthcare, retail
- **CTI League:** Volunteering as a Darknet researcher, creating crawlers and scrapers to scrape from the darknet for monitoring healthcare threats
- **StationX:** Volunteering as a Teaching Assistant, moderating the discourse, engaging with the community, and solving security course-related doubts

SKILLS

- **Programming:** Proficient in Python and Bash, Knowledge of C, C++, Java, Assembly (x86)
- **Security:** Threat Intelligence, Threat Hunting, OSINT, SOCMINT, HUMINT, Reverse Engineering, Malware Analysis
- **Tools:** Elasticsearch, Kibana, Splunk, Yara, GDB, Ghidra, IDA Pro
- **Miscellaneous:** Elastic Stack (ELK), MITRE ATT&CK, NLP, SIEM, TIP

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

- **Blue Team Level 1 by Security Blue Team:** (Ongoing)
- **Threat Hunter Battle Path by Rangeforce:** (Ongoing)
- **Fundamentals of Cyber Investigations and Human Intelligence workshop by Christina Lekati and Samuel Lolagar:** (Feb 2021)
- **SOC Analyst 1 Battle Path by Rangeforce:** (Jan 2021)
- **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 ATT&CK (16-hour) by John Strand:** (Jul 2020) [\[Link\]](#)
- **CompTIA Security+ ce by CompTIA:** (Feb 2019 - Feb 2022) [\[Link\]](#)