Rhyme Upadhyaya

rhyme.u7@gmail.com
+91 99559 72503
linkedin.com/in/rhymeu

Summary

- Experienced Cyber Security Researcher with 4.5 + years of relevance to work in CyberSec & strong team management skills

- Crux : A WhiteHat with super specialisation in dissecting malwares, Malware Forensics, Reverse Engineering with knowledge in x86, x64, ARM, Network Security and Cyber Security Operations

- Malware Analysis skills in platforms: Windows, MAC, Linux

- Highlights : Virus / Worm / Trojan / Exploit / PUA signatures, YARA, Honeypots, Threat Intelligence / Hunting, APT, Live attack Infrastructure, IDS / IPS

- Deep Web research and automation, Powershell automation and fileless malwares, Enumeration, whitelisting / blacklisting

- Python and data science, Applied Machine Learning in malware analysis, Quantum Computing

- VAPT, Secure code review

- Technical Writing, IOT Security, Wi-Fi Security, Application Security

Experience

Assistant Manager

Aug 2019- Present

Price Waterhouse Coopers (PWC)

Leading the Digital & Malware Forensics team in CyberSecurity division of PwC.

Professional Freelancer

Nov 2016- Present

Confidential

I Freelance with educational websites and few organisations under a NDA

- Technical Content Writing & creating quizzes / assessments
- Threat Intelligence
- Product testing
- Digital Rights management
- Dark web research
- Blockchain development
- Digital Marketing [Search Engine Optimization]

Threat Researcher

Mar 2018 - Jul 2019

Sophos Labs

1 year 5 months

- Virus / Worm / Trojan signature writer / reviewer [Language : VDL]
- Author into internal Sophos Wikipedia

- Publishing Threat Description onto Sophos Labs knowledge Base
- Malware Research & Response
- Imparting internal training [PE / Non PE / Script based Malwares]
- Handling premium accounts, OEMs, privileged Cx escalations
- URI Ops [Website audits and penetrating testing]
- Handling Frontline escalations
- Handling False positives & False negatives
- Whitelisting / blacklisting Digicerts of trusted / untrusted vendors
- Covering PUAs
- Compliance testing with senior team members from Vancouver Labs, CA
- Products : SAV, Invincea, Cryptoguard, Central, SEC
- Work closely with the Security Operations Center (SOC) and IDS / IPS team on threat hunting / Response
- Work closely with the Data Science team in testing out models for successful integrating onto products
- Beta testing with the System development team in Hungary.
- Handle alert management with tools like SPLUNK & ARCSIGHT
- Writing Application Control covers
- Knowledge on vectors & elements like Opsgenie, VictorOps, JIRA, AWS, MITRE, Kill Chain, Diamond Model, STIX, TAXII, RegEx

Information Security Consultant

Feb 2017 - Feb 2018

SEQURETEK

1 year 1 month

- Writing YARA for development of their security solution
- Threat Hunting & Threat Intelligence / APT
- Malware Forensics & Repository automation
- Deploying Honeypots
- Deep Web Research
- Imparting training to a team of Consultants / freshers
- Python based Web Scraper for a known financial institution
- Active Directory Configuration & Control
- Process Enumeration & Scheduling
- Joomla based internal knowledge base
- Designing advanced security solutions with the development team
- Working closely with Security Operations Center (SOC) to automate feeds

Information Security Associate

Jul 2016 - Feb 2017

CR Risk Advisory

8 months

- Offensive Security Research [NDA : 3 Years]
- Worked closely with IDS / IPS feeds and PCAP analysis to write signatures for coverage in their security solution
- Imparting training to team
- Crime Investigation and risk mitigation techniques
- Website audits
- Link analysis
- Designing Spam traps and auditing for a secure internal infra

Masters Research Associate

Jul 2015 - Aug 2016

Birla Institute of Technology, Mesra

1 year 2 months

Mtech (By Research) from one of the oldest engineering colleges of India.

Responsibilities in understated Labs undertaken as a research associate :

- **Operating systems**, **C**, **Cryptography** & **Network Security**

Dissertation

- Behavioral Classification of **CTB Locker ransomware** and detection through Hybrid analysis
- **Research** awarded a **CGPA (10) for 2 consecutive semesters** and **least plagiarism [3%]** in entire batch

- **IEEE** publication and speaker at conferences

Intern

Sep 2013 - Apr 2014

ISOEH

8 months

Cyber Security Intern

Highlights : Malware Research & Reverse Engineering

Education

Birla Institute of Technology

2014 - 2016

Master’s Degree, Mtech(Computer and Information Systems Security), 1st Div

1st Division with Distinction specialising in Cyber Security

Interests :

- Cryptography & Network Security
- Biometric Security
- Database Security
- Security Operations Research with C programming
- Optimization Techniques
- Mobile communication
- Networking

West Bengal University of Technology, Kolkata

2009 - 2013

Bachelor’s Degree, Btech (Information Technology), 1st div

Specialization has been Information Technology with a knack in following **modules** :

- Cryptography
- Networking
- Programming [C, C#, Java]
- Operating Systems
- Multimedia
- Artificial Intelligence

Internship & Project(s)

- Employee management system
- E-tutoring system [Mamdani rule backed]
- Smart shopping mall [ecommerce website]
- Library management system

Skills

Malware Analysis • Reverse Engineering • Vulnerability Assessment • Penetration Testing • Machine Learning • Python (Programming Language) • Deep Web Research • CGI/Perl • x86 Assembly • Artificial Intelligence (AI)

Certifications

Certified Ethical Hacker v9 • EC-Council

ECC96331741588 • Feb 2017 - Feb 2020

Script based malware signature reviewer • Sophos Anti-Virus Labs

PE & Non PE malware signature reviewer • Sophos Anti-Virus Labs

Script based malware signature author • Sophos Ani-Virus Labs

PE & Non-PE malware signature Author • Sophos Anti-Virus Labs

Nominum (Cisco) certified Analyst / Reviewer • Sophos Anti-Virus Labs

Malware Analysis & Reverse Engineering • Sophos Anti-Virus Labs

Spam Analyst • Sophos Anti-Virus Labs

Network Intrusion Analysis • Concise Courses(Florida,USA)

Honors & Awards

- **Anandaram Barua Award for Academic Excellence** • Govt. Of Assam • Mar 2008

Award for achieving excellent scores in 5 consecutive subjects comprising Math, Science and literature papers along with World history with star marks.