SURAJ YADAV

Security Researcher

suraj372y@gmail.com | +91-6395090849 | 0xk4n3ki.github.io | k4n3ki | 0xk4n3ki

EXPERIENCE

Security Research Intern

Cyble Inc.

June 2024 – Sep 2024 | Bangalore

- Analyzed 50–100 malware samples daily via VirusTotal and performed static and dynamic analysis on emerging threats—such as OpenAI Sora and Zoom-themed phishing campaigns delivering stealers and RATs—identifying novel variants and APT activity
- Compiled 10+ weekly vulnerability intelligence reports for BFSI clients, covering critical CVEs, Linux malware trends, brute-force activity, and IoCs (IPs, hashes, email addresses); enriched insights using Kibana (Elasticsearch) and T-POT honeypots to support incident response
- Investigated 100–200 high-risk domains daily, shortlisted using a custom script from 50,000+ newly registered domains, to uncover phishing infrastructure and active malware distribution; flagged brand impersonation domains to enable swift mitigation
- Authored 40+ daily security advisories on zero-days, emerging threats, and data breaches—delivered to internal stakeholders and clients to enable real-time threat mitigation and strengthen overall security posture

Cloud Security Research Intern

Cloud Security Club

May 2024 – June 2024 | Remote

- Utilized AWS security best practices by managing EC2, S3, IAM, and Lambda; identified and remediated cloud misconfigurations to mitigate potential exploitation
- Developed comprehensive, step-by-step security guides on AWS misconfigurations and best practices on flaws.cloud, flaws2.cloud, and Cloudgoat to educate the community and enhance incident readiness

PROJECTS

Shellcode Injector

- Engineered a C++ proof-of-concept Windows shellcode injector employing API hashing and manual PEB parsing to evade antivirus detection—demonstrating offensive security techniques and an adversarial mindset

PE Parser

- Created a robust C++ based PE parser for Windows 32-bit executables, extracting headers, sections, imports, and exports to support malware reverse engineering and forensic analysis

EDUCATION

Bachelor of Technology

Indian Institute of Technology Roorkee

Nov 2020 – May 2024

BLOGS & PUBLICATIONS

0xk4n3ki.github.io – Personal Blog

- Developed a platform for publishing blogs on malware analysis, reverse engineering, binary analysis, digital forensics, CTF writeups and DevOps
- Analyzed multiple real-world malware samples including Luckbit ransomware, Agentb Trojan, and Dridex stealer

CAMPUS ENGAGEMENT

CTF Player @InfoSecIITR

Sep 2021 – March 2023

- Achieved 1st place in CSAW CTF India Finals and 3rd in JadeCTF 2022; contributed to InfoSecIITR's ranking as #2 in India on the CTFtime leaderboard
- Led and supported campus cybersecurity initiatives by organizing Backdoor CTF and NoobCTF, and conducting hands-on workshops for peers

- Joint Secretary, Himalayan Explorer Club – led treks & eco-drives
- Video Editor, onRec – managed junior team, produced podcast for Class of 2022

STRENGTHS

Malware Analysis | Incident Response | Exploit Dev | Vulnerability Management

C/C++ | Python | Go | Malware Analysis | IDA | x64dbg | DiE | gdb | angr | Wireshark | Procmon | Burpsuite | FTK Imager | Autopsy | Git | Docker | Jenkins | Kubernetes | AWS | Elasticsearch