Samdup Choephel

samchoe2002@gmail.com | linkedin.com/in/samdupc | tcert.net | github.com/samduk | Himachal Pradesh, India

Malware Analyst and Reverse Engineer with 4+ years defending high-risk organizations against nation-state APT threats.
M.S. Cybersecurity, Georgia Tech (2024) | Fulbright Scholar | Actively deepening analysis depth via FOR610 curriculum.

TECHNICAL SKILLS

Analysis & RE: Ghidra, x64dbg, CAPE Sandbox, FLARE VM, PE-Bear, INetSim, YARA, Wireshark
Blue Team / IR: SIEM triage, memory forensics, iptables, Cloudflare, fail2ban, mod_security, log analysis
Programming / Scripting: Python, Bash, C/C++ (Comprehending), PHP, SQL
Languages: English (fluent), Tibetan (fluent), Hindi (intermediate), Chinese (conversational)

EXPERIENCE

SOC / Malware Analyst | *Central Tibetan Administration, TCRC* Aug 2024 - Aug 2025

- Triaged SIEM alerts daily; analyzed 5-20+ samples/month (PE, DLL, Office, PDF, phishing) using Ghidra, x64dbg, and CAPE Sandbox with formal IOC and YARA reports delivered within 24 hours.
- Led 8-day incident response against a sustained politically-motivated DDoS: performed payload analysis to de-anonymize coordinated attack sources despite IP randomization; restored service via iptables, Cloudflare, and fail2ban.
- Automated static-analysis triage of Office and media files with Python and Bash scripts, reducing analyst workload on repetitive pre-processing tasks.
- Mentored 10+ cybersecurity interns on APT research targeting the Tibetan exile community; supervised live penetration testing engagements and delivered server hardening and log analysis training to technical staff.

Malware Analyst | *Central Tibetan Administration, TCRC* Aug 2021 - Jul 2022

- Analyzed 3-20+ samples/month; investigated staged loader using PDF OpenAction and scheduled task persistence; simulated C2 with INetSim to identify download targets and payload types.
- Uncovered fake AVAST browser persisting across reboots via deeply embedded mechanisms; traced C2 to endpoints in Malaysia and Hong Kong through network behavioral analysis.

Penetration Tester and Incident Responder | *Central Tibetan Administration, TCRC* Jul 2020 - Aug 2021

- Performed pre-launch black-box assessments of internal CTA applications; discovered and coordinated remediation of a critical vulnerability in a third-party outsourced system.
- Conducted memory forensics on suspected machines; produced structured IR reports enabling independent machine recovery by technical staff.

Founder / Security Lead | *ePotala (pro-bono infosec for Tibetan NGOs)* Feb 2014 - Jan 2021

- Recovered the Tibetan Parliament in Exile website from active compromise (2015): collected and analyzed PHP webshells, attributed attack to Hong Kong IP via log forensics, and hardened server against reinfection.
- Provided election-cycle security for the Tibetan Election Commission (2020): deployed iptables, fail2ban, mod_security, and custom log-analysis scripts to block crawlers and mitigate DDoS.

Graduate Teaching Assistant | *Georgia Institute of Technology, ECE4150 Cloud Computing* Jan - May 2024

- Supported instruction for 120+ students; held office hours and served as the primary student contact for technical and academic queries.

Webmaster and System Administrator | *Tibetan Centre for Human Rights and Democracy* May 2015 - Apr 2016

- Built three multilingual sites (English, Tibetan, Chinese) with custom PHP/MySQL backend; hardened WordPress and Linux servers; implemented secure communication channels for researchers handling sensitive human rights data.

EDUCATION

M.S. Cybersecurity, Information Security Track Georgia Institute of Technology May 2024
M.Sc. Computer Science St. Joseph's College, Bangalore 2013

TRAINING, CERTIFICATIONS AND RECOGNITION

Actively studying: FOR610 Reverse-Engineering Malware curriculum (open-source materials), GIAC GREM in preparation
CTF / Labs: TryHackMe Top 5% (100+ machines), crackmes.one binary reversals
Trainer: Internet Freedom Festival, Valencia (2018, 2019) - Malware Hunting and Packet Analysis | COCONET Southeast Asia Digital Rights Workshop, Indonesia (2017) - Web App Attacks
Scholarship: 2022 Tibetan Scholarship Program, US Bureau of Educational and Cultural Affairs (Fulbright) for Georgia Tech