Son Tung Thuong

10-03-2005 | Anaheim, California | sontung346@gmail.com | My Linkedin | My Portfolio

About me

I am a third-year Information Security student from Vietnam, passionate about uncovering cyber threats through **Threat Hunting**, **Threat Intelligence**, **Digital Forensics**, **Incident Response**, and **Malware Analysis**. I actively compete in CTFs and explore real-world attack simulations to build practical skills.
I aim to join a **professional SOC or DFIR, CTI, Malware Analysis team** as an intern, where I can both learn and contribute—whether it's analyzing incidents, responding to threats, or hunting adversary behaviors in complex environments.

Certifications

- **Ethical Hacker** – click to view more
- **Google Cybersecurity Certificate** – click to view more

Education

Posts and Telecommunications Institute of Technology, Ho Chi Minh City — Aug 2023 – May 2025

- **Cumulative GPA: 3.04/4.0** (Engineering degree in Information Security)
  - *Coursework:* Linear Algebra, Calculus 1-2, Computer Architecture, Object Oriented Programming, Data Structure & Algorithm, Computer Networking.
- **Class Monitor** – Led academic coordination and student activities for a class of 60 students for 3 consecutive years
- **3rd Place – PTITHCM CTF 2024** which held by PTITHCM
- **1st Place – PTITHCM CTF 2025** which held by PTITHCM
- Engaged in cybersecurity communities, workshops, and hands-on labs in malware analysis and digital forensics.
- Monitoring and developing DFIR challenges for PISCTF - a cyber security competition for PTITHCM's students only.

Project

- Unpacking APT32 Campaign: KorPlug RAT disguised as antivirus
- Retrieving plaintext KeePass database password in Memory Forensics using Windbg
- Malware hunting in Memory Forensics with cracking TLS v1.2 traffic to decrypt C2 communication

Technical Skills

- **Threat Detection & Incident Response**: Cross-platform forensics (Windows/Linux/macOS/Android/iOS), memory/disk/log analysis (Volatility, FTK, Autopsy, Sysmon, EZ Tools), threat intel with OSINT tools (Shodan, Sherlock, holehe) and platforms (VirusTotal, MalwareBazaar, Any.run,...).
- **Threat Hunting**: Using Splunk to continuously monitor, analyze, detect and hunt suspicious or malicious behavior across systems, applications, and networks.
- **Malware Analysis**: Ability to detect malware evasion techniques (DLL Injection, Registry Tampering, Reflective DLL).
  Static (IDA Pro, Ghidra, dnSpy) & Dynamic (strace, Wireshark, Any.run) analysis on PE/ELF in C/C++, .NET, ASM, Python.
- **Tools & Techniques**: Sysinternals, Splunk, Wazuh, Wireshark. Integrated RE for IOC extraction.
- **Capture The Flag (CTF)**:
  - Team leader of **f4n_n3r0**, currently ranked 1st in Vietnam and 7th in the world on CTFtime.org
  - Member of **L3AK**, a top-tier international CTF team.
  - Actively compete in CTFs with a focus on Forensics, Reverse Engineering, OSINT and low-level system

challenges.
  - **Top 1** - 0xL4ughCTF 2026 (With L3ak)
  - **Top 6** - KnightCTF 2026 (Hosted by the Knight Squad community from Bangladesh)
  - **Top 1 –** CyberMaterial HackHavoc CTF (Hosted by CyberMaterial)
  - **Top 3 - 2nd runner-up** - ASEAN Open CTF (Hosted by ASEAN-Japan Cybersecurity Capacity Building Center - Individuals only)
  - **Top 10** - BOTSv9 Mongolia (Boss of The SOC - Hosted by Splunk)
  - **Top 42 out of 7067 teams** - HackTheBox Holmes CTF - Blue Team only CTF
  - **Top 7 - Merit Prize –** Hacktheon Sejong 2025 Finals (Hosted by Sejong City)
  - **Top 7** - World Wide CTF 2025 (Hosted by World Wide Flag CTF team)
  - **Top 1 –** Cygenix CTF (Hosted by Cybergenix Security)
  - **Top 23 –** Black Hat USA CTF (Hosted by Bugcrowd)
  - **Top 11** - Kashi CTF 2025 (Hosted by BHU CyberSec)
  - **Top 9** - VishwaCTF 2025 (Hosted by CyberCell VIIT)
  - **Top 6** - ApoorvCTF 2025 (Hosted by Cybersecurity Club, IIIT Kottayam)

- **Programming**:
  - Proficient in C/C++, Python and Powershell for automating forensic workflows, parsing logs and PCAPs, and decoding/decrypting data during incident investigations.
  - Basic DSA / Encryption / Cryptography techniques: Sort/Search, AES, RC4, RSA.

Soft Skills

- **Technical Communication**:
  - Explained complex DFIR and Threat Hunting concepts to non-technical teammates through clear, concise writeups and debriefs.
  - Documented key forensic findings and investigation steps in case reports, including screenshots, tool outputs, and timeline analysis.
- **Collaboration & Leadership**:
  - Led a 4-member CTF team to top 10 finish by coordinating roles (RE, crypto, forensics, pwn, web, OSINT)
  - Resolved conflicts during group projects by aligning technical approaches with shared goals
- **Problem-Solving Mindset**:
  - Investigated security incidents by performing forensic triage, timeline reconstruction, and disk/memory artifact extraction.
  - Analyzed unusual file/system behaviors (e.g., tampered logs, modified headers) to trace attacker footprints and persistence techniques.