NGUYEN QUANG HUY

SECURITY ENGINEER

CONTACT

+84-327-739-497

reisen1943.ctf@gmail.com

Binh Thanh District, HCMC

anduinbrian.github.io

https://github.com/AnduinBrian

EDUCATION

2015 - 2020

POSTS AND TELECOMMUNICATIONS INSTITUTE OF TECHNOLOGY

- Security Engineer

SKILLS

- Programming Language:
  - C/C++
  - Python
  - Assembly
- Reverse Engineering
- Exploit Development
- Using SRE tool:
  - Decompiler: IDA, Ghidra, JADX,...
  - Debugger: x64dbg, gdb

LANGUAGES

- Vietnamese
- English

WORK EXPERIENCE

Asia Commercial Joint Stock Bank 2023 - PRESENT

SOC Analyst/Threat Intelligence

- Build and maintain an IoCs auto-collector using MISP and VirusTotal/OTX combined with a SandBox (based on CAPEv2) to extract malware's IoCs.
- Monitor and process alerts for malware, promptly responding to potential threats detected.
- Create a report on malware, covering its types, behaviors, impact on systems, common infection vectors, evolution, notable attacks, and strategies for prevention and mitigation.
- Analyze the phishing email and warn the user.
- Build and maintain a system to collect all information about leaked accounts.
- Develop a custom loader to bypass antivirus software to support red team operations.
- Install and manage an ESXi server to provide virtual machines for testing exploits.
- Analyze and reproduce publicly disclosed vulnerabilities on Linux.

VinCSS 2022 - 2023

Incident Response

- Verify incident alerts to assess and address potential security threats.
- Perform forensic analysis on the infected machine to gather evidence, identify malware.
- Analyze malware and extract IoCs and develop a specialized tool to remove malware from infected systems.
- Hunting malware on VirusTotal/Any.Run involves uploading samples, analyzing behavior, extracting IOCs.
- Verify the abnormal email by its content, headers, and attachments to assess threats.

Armor Security 2019 - 2022

Malware analyst

- Analyzing malware on VirusTotal/Any.Run, tracking trends, and sharing insights for emerging threats and mitigation.
- Report on malware attacks targeting Vietnamese internet users, detailing types, impacts.
- Monitoring and documenting advanced persistent threat (APT) group activities targeting Vietnam, analyzing tactics and impacts.
- Scrutinize for any malware in the company's system.

SIDE-PROJECT

- I do research on automotive, hardware, RF and IoT in my free time:
  - **Journey with Totolink router** - Finding vuln on the T6 router. *(https://github.com/AnduinBrian/https://anduinbrian.github.io/posts/blogs/totolink-t6-v3/)*
  - **About ADS-B** - Learn about the ADS-B protocol, capture and extract info from it. *(https://anduinbrian.github.io/posts/blogs/about-ads-b/)*

- I play CTF with "**CTF Academy**" Team, mentored by **Shellphish**:
  - **bi0sCTF 2025** - Writeup about CAN Bus challenges. (*https://anduinbrian.github.io/posts/writeups/bi0sctf---2025/*)
  - **Practical Car Hacking** - Writeup about basic task in car hacking. (*https://anduinbrian.github.io/posts/writeups/practical-car-hacking-ctf/*)

ACHIEVEMENT

The Flare-on Challenge 2024
- Participate and finish the Flare-on Challenge.
- *Username: Reisen_1943*

The Flare-on Challenge 2023
- Participate and finish the Flare-on Challenge.
- *Username: Reisen_1943*

The Flare-on Challenge 2022
- Participate and finish the Flare-on Challenge.
- *Username: Reisen_1943*

pwn.college
- Obtain: Orange Belt | Yellow Belt | Green Belt | Blue Belt
- *Username: Reisen_1943*

CVEs
- **Totolink T6:**
  - ***CVE-2025-6916***: Login bypass.
  - ***CVE-2025-7862:*** Missing authen.
  - ***CVE-2025-7758***: Stack buffer overflow in CGI.
  - ***CVE-2025-7837:*** Stack buffer overflow in MQTT service.
  - ***CVE-2025-7862***: Stack buffer overflow in MQTT service.
  - ***CVE-2025-7912:*** Stack buffer overflow in MQTT service.
  - ***CVE-2025-7913***: Stack buffer overflow in MQTT service.