NGUYEN QUANG HUY

SECURITY ENGINEER

CONTACT

+84-327-739-497

reisen1943.ctf@gmail.com

Binh Thanh District, HCMC

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 mantaince 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.

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.

PERSONAL PROJECT

- loader (*https://github.com/AnduinBrian/loader*): A loader designed to execute custom shellcode, capable of evading detection by TrendMicro EDR.
- firm_find (*https://github.com/AnduinBrian/firm_find*): A compact Python script designed to search for files of interest or importance in the squashfs root directory. It supports my research on IoT bugs.
- malware_adventure (*https://github.com/AnduinBrian/malware_adventure*): My personal malware analyst blog.
- auto_vt (*https://github.com/AnduinBrian/auto_vt*): A Python library to fetch the newest IoCs from VirusTotal and verify them using OTX.

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

- Orange + yellow + green belt
- Username: Reisen_1943

CVEs:

- CVE-2024-10654 - formAuthLogin bypass
  - https://github.com/c0nyy/IoT_vuln/blob/main/TOTOLINK%20LR350%20Vuln.md