Ryo Ichikawa

icchyr@gmail.com github.com/icchy

Skills

- Programming Languages: C/C++, Python, Go
- Systems: Linux, Windows (Forensics), Hypervisor (BitVisor)

Work experience

- Nov. 2018 - Present, National Institute of Advanced Industrial Science and Technology
- Apr. 2018 - Oct. 2018, Arizona State University (Intern, Research Specialist)
- Mar. 2015 - Present, Cyber Defense Institute, Inc. (Forensic Analyst)
    - Analyzed Linux and Windows malware
    - Wrote a forensic tool for parsing NTFS MFTs
    - Developed a data collection tool for initial response
- Sep. 2017 - Oct. 2017, NTT Secure Platform Laboratories. (Security Research Intern)

Activities

CTF: TokyoWesterns CTF team founder/captain

- Ranked 4th in the world as of 2018 (https://ctftime.org/team/12599)
- Notable on-site results
    - 2nd place, WCTF 2017, Beijing (http://ctf.360.cn/en/index.html)
    - 1st place, WCTF 2018, Beijing
    - 4th place, Google Capture the Flag 2018 (Finals), London

Talks

- "New Frontier of CTF - Bull's Eye", NDSS Workshop on Binary Analysis Research 2019, San Diego
- "Let's Make Windows Defender Angry: Antivirus can be an oracle!", CODE BLUE 2019, Tokyo, Japan

Hosted CTFs

- TokyoWesterns CTF (https://ctftime.org/ctf/116)
- CODE BLUE CTF (co-hosted) (https://ctftime.org/ctf/208)

ACM-ICPC: team "nocow" from Tokyo University of Agriculture and Technology

- 5th place, 2017 Japan Domestic
- 8th place, 2017 Thailand Nakhon Phatom

ISUCON: Speeding up contest for web application

- 1st place, 2018 Finals, Japan

Writing Tools

- Windows API tracer for malware analysis (https://github.com/icchy/tracecorn)
- PE parser from scratch in Python (https://github.com/icchy/pe)

Education

- Apr. 2017 - Mar. 2020, Master of Computer Science, Tokyo University of Agriculture and Technology
- Apr. 2013 - Mar. 2017, Bachelor of Engineering, Tokyo University of Agriculture and Technology

Research

- Monitoring guest OSes from a thin hypervisor programmatically
    - resolving the semantic gap with LibVMI, porting Lua and LibVMI to BitVisor
- Fuzztainer: fuzzing real-world docker containers parallelly
- Kernel size reduction by analyzing linux binaries
- Graduate thesis: Efficient OS Monitor Based on Thin-Hypervisor with Built-in Interpreter Programming Language